



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Deploying Zope and Plone portals

A low cost solution

*R. Carbone
DRDC Valcartier*

Defence R&D Canada – Valcartier

Technical Note

DRDC Valcartier TN 2006-585

October 2006

Canada

Deploying Zope and Plone portals

A low cost solution

R. Carbone
DRDC Valcartier

Defence R&D Canada – Valcartier

Technical Note

DRDC Valcartier TN 2006-585

October 2006

Principal Author

Richard Carbone
Programmer/Analyst

Approved by

Yves van Chestein
Head/Information and Knowledge Management

© Her Majesty the Queen as represented by the Minister of National Defence, 2006

© Sa Majesté la Reine, représentée par le ministre de la Défense nationale, 2006

Abstract

In Summer 2005 a task was undertaken to build and implement a rapid portal deployment environment based on a content management system. DRDC projects such as MSOC and ARMADA have seen and reaped the benefit of utilizing portal-based environments. The objective was to implement such a portal based on readily available open source products in order to reduce the costs and yet benefit from a highly configurable, flexible, robust, and low-cost solution. The current portal described in this document is supporting both internal DRDC clients as well as international clients via the TTCP. The main objective of this document is to share the experiences of implementing just such a portal and describe how to build and rapidly deploy one. It also presents how to ensure due diligence with respect to its security.

This page intentionally left blank.

Executive summary

Deploying Zope and Plone portals: A low cost solution

Carbone, R.; DRDC Valcartier TN 2006-585; Defence R&D Canada – Valcartier; October 2006.

DRDC projects such as Knowledge Management for Marine Security Operation Centres (KM4MSOC) and ARMADA require a Content Management System (CMS) in order to share information in a timely manner with other users and ensure that there will be no documentation duplication. Thus, a rapid portal deployment environment utilizing [Zope](#) and [Plone](#) was required in order to provide an effective method for performing network CMS and portal-based collaboration via a centralized portal. With this portal, scientists from different DRDC facilities can become involved and work on documents and share information with their counterparts in a network-centric environment.

The significance of the work was to demonstrate that it is possible to quickly build and deploy a network-based portal environment. The steps and procedures are easy to follow as is the installation and configuration so that users and organizations can quickly build, deploy, and maintain their own portal cheaply using readily available open source products. It is important to document these steps as the process can reduce the complexity and costs associated to procuring commercially available solutions that sell for tens of thousands of dollars. With minimal effort from the user, it is possible to realize enormous cost savings and deploy an effective portal environment. Furthermore, it is becoming standard procedure within the Knowledge Management Systems Group (KMSG) at DRDC Valcartier to deploy a portal prior to any new research project commencing. Thus far, two portals have been implemented, one for internal use among the various DRDC facilities and the other for use by international counterparts.

However, due to the fact that networks available to CF users are DWAN and CNET. These networks are run under a tight configuration and deployment policy. While deploying open source tools and portals may be a rather simple objective, it is important to first permission to do so and an impact assessment report should be done as well. The reliability and complexity of DWAN and CNET could be compromised if users attempt to perform unauthorized actions on these networks (i.e. deploying open source software) without adequate safeguards in place.

This page intentionally left blank.

Table of contents

Abstract	i
Executive summary	iii
Table of contents	v
List of figures	vii
List of tables	viii
Acknowledgements	ix
1. Standard Implementation	1
1.1 Introduction	1
1.2 Basic setup.....	1
1.3 Obtaining the necessary packages and add-ons.....	3
1.4 Installing Zope and subsystems.....	3
1.5 Creating the Plone site.....	8
1.6 Configuring WebDAV	11
1.7 Setting up the virtual host.....	12
1.8 Securing the portal system.....	14
1.8.1 Disabling system services	14
1.8.2 Configuring the security scanner	15
1.8.3 Running the security scanner	17
1.9 Wrap up	19
2. Optional component implementation.....	20
2.1 Implementing mail redirection	20
2.2 Setting up SSL.....	20
2.2.1 Introduction.....	20
2.2.2 Creating a signed SSL key/certificate	21
2.2.3 Configuring SSL virtual hosting	22
2.2.4 Miscellaneous.....	24
3. Conclusion	25
References	26
Annex A System configurations, tests, and outputs	27
A.1 Verbose Zope start-up output detailing optional tools and features	27
A.2 File contents of httpd.conf	30
A.3 File contents of ssl.conf	38
Annex B Nessus security scan report	40
B.1 Part I of the Nessus report.....	40
B.2 Part II of the Nessus report.....	42
Bibliography	160

List of symbols/abbreviations/acronyms/initialisms	161
Glossary.....	163

List of figures

Figure 1. Logging in to Zope.....	5
Figure 2. The ZMI and other configurable options	6
Figure 3. Fields and sample data required for creating a new Plone site	9
Figure 4. The newly-created Plone site	10
Figure 5. The new Plone site “test2”	11
Figure 6. Example of virtual hosting without specifying port 8080 to access the Plone site	14
Figure 7. Example of user-configurable features via the Nessus client interface.....	18
Figure 8. Accepting a certificate signed by an unknown authority	24

List of tables

Table 1. Disk partitioning for the disk during installation.....	2
Table 2. Values used for creating a new Plone site	8
Table 3. Fields and values for creating Nessus certificate.....	17

Acknowledgements

The author would like to thank Martin Salois for his hard work in revising this document to ensure its accuracy and relevancy. The author would also like to thank Dr. Alain Auger in revising the final version of this document.

This page intentionally left blank.

1. Standard Implementation

1.1 Introduction

During the process of building a CMS rapid portal deployment environment, it was decided to document all of the steps and procedures and share them with those that would be interested in doing the same. The steps and procedures found in this document are written to help demonstrate to others how to deploy a portal system similar to the one built at DRDC. Key background information has been included to help put things into perspective and to aid in clarification. Portal systems are rapidly finding place and acceptance in today's field of knowledge management and thus were considered appropriate for use in certain DRDC projects.

It is because of the requirements of projects such as MSOC and ARMADA that a portal environment was implemented. A short amount of time was available to do so and budgetary constraints were prevalent. Commercial-based portal systems can easily cost several tens of thousands of dollars. Furthermore, resources for maintenance and support of the deployed portal system were scarce.

Looking at various open source technologies, it was determined that not only could a robust portal environment be deployed for very little cost and manpower but that such a system could also be easily maintained via updates, patches, fixes, kernel upgrades, etc.

The main objective of this document is to share the experiences of implementing just such a portal and describe how to build and rapidly deploy one. It also presents how to ensure due diligence with respect to its security.

There are now currently two such portal systems deployed at DRDC Valcartier. One system is accessible via the corporate network, and the other is available via the Internet. Both systems are in current use by both DRDC personnel and by international colleagues.

N.B.: However, due to the fact that networks available to CF users are DWAN and CNET. These networks are run under a tight configuration and deployment policy. While deploying open source tools and portals may be a rather simple objective, it is important to first permission to do so and an impact assessment report should be done as well. The reliability and complexity of DWAN and CNET could be compromised if users attempt to perform unauthorized actions on these networks (i.e. deploying open source software) without adequate safeguards in place.

1.2 Basic setup

Before implementing [Zope](#) or [Plone](#), the [Linux](#) operating system must already be installed and functional. There are many different distributions of [Linux](#) to choose from; through trial and error, it was found that one best suited to [Zope](#) and [Plone](#) was [Fedora Core 3 \(FC3\)](#). At this time, there are versions of [Fedora Core](#) that are more recent than the one used for the portal system. The portal system utilizes [FC3](#). It installs and works very well on a Pentium III with 512 MB RAM and a 20 GB disk. This is the configuration of the system used to build the [KMSG] rapid

portal deployment environment. Memory size can vary depending on the size of the portal. Generally, the larger the portal the more memory required.

Before actually installing [Fedora Core Linux](#), it is important to choose the most recent version of that distribution. Choosing a recent distribution will significantly reduce the work required to perform a system update and save time when fixing security issues found during the security audit.

Installing [FC3](#) is a rather simple task. A full installation will consist of more than 1,000 packages. Nevertheless, it is suggested to install them all. This is in order to avoid any potential library or interdependency problems. The system's disk was partitioned as follows:

Table 1. Disk partitioning for the disk during installation

Disk	Disk Size (in GB)	Mount Point	Partition Size (in GB)
1	20	Swap	1.5
1	20	/boot	1.0
1	20	/	17.5

The disk was partitioned using the [Disk Druid](#) utility that is a part of the [FC3](#) distribution. The installation on a Pentium III takes just over one hour to complete from start to finish. Note that the ratio¹ of physical RAM (512 MB) to swap size (1.5 GB) is 3:1, and the distribution installation size of 6.0 GB to root partition size is also about 3:1. This ratio will help to ensure optimal performance of memory, swap, and adequate disk space.

Network information (i.e. IP address, netmask, etc.) should already be available prior to installation. If it is not available, it can be configured later on using other means.

The installation did not require an active firewall since the corporate sandbox² (where the system would ultimately be placed) would take care of these issues. [SELinux](#) was not enabled since no classified information was to be used under the auspice of the portal system.

The required TCP/IP information was obtained from corporate network services. A static address of 143.146.253.7/255.255.255.0 was provided including DNS server, mail server, and network gateway information. The system's static IP configuration can be found in `/etc/sysconfig/network-scripts/ifcfg-eth0`. Name resolution is provided by DNS. Its configuration file `/etc/resolv.conf` should appear similar to the following:

¹ [Linux](#) is well known to work well with a ratio of about 3:1 for swap to RAM, operating system to disk space, etc.

² The sandbox is a special sub-network which can be made available to the Internet at large. However, most of the network ports are completely disabled on the network's Internet-connected router.

```
nameserver1 143.142.16.30
nameserver2 143.142.1.30
search drdc.dnd.ca
```

DNS name resolution helps in tracking and logging which remote systems connect to the portal.

At this point, networking should be appropriately configured. However, the system itself should not yet be connected to any network; it should be left stand-alone until placed in the sandbox.

1.3 Obtaining the necessary packages and add-ons

The required packages and add-ons should be downloaded from an Internet-connected workstation and then copied over to the portal system via removable media. At the time of writing, the current [Zope](#) RPM package (Red Hat Package Manager) was at version *2.75-1.fc3.i386*. This is a binary package and not in source code format. All of the other packages, by contrast, were source code packages. The source code package for [Plone](#) was *Plone-2.0.5.tar.gz*. The add-on source code packages that were downloaded are [TextIndexNG](#) 2.2.0, [Catdoc](#) 0.94, and [WV](#) 1.0.3. Their corresponding filenames are *TextIndexNG-2.2.0b2.tar.gz*, *catdoc-0.94.tar.gz*, and *wv-1.0.3.tar.gz*, respectively.

[WV](#) is a series of tools and libraries that provide WMF ([Windows](#) Metafile) capabilities to [Plone](#). [TextIndexNG](#) provides text indexing tools for [Plone](#) that recognize various text editing formats such as MS [Word](#), PDF (Portable Document Format), and others. [Catdoc](#) is a tool that converts MS [Office](#) files into various useful formats such as CSV (Comma Separated Value).

Once the files have been downloaded, they are to be copied over to the portal system and placed in a newly created directory */root/zope*. This will be the new portal software repository.

1.4 Installing Zope and subsystems

Once the various downloaded software components have been copied to the portal system under */root/zope* they can be installed and compiled. There is a specific order, described here, for installing the software packages. To install the [Zope](#) RPM package, execute the following commands as the portal system's root user:

```
$ cd /root/zope
$ rpm -i zope-2.7.5-1.fc3.i386.rpm
```

The [RPM](#) program installs the [Zope](#) package. Once complete, changes to the system password file (*/etc/passwd*) are in order. A new user "zope" must be added and a new directory hierarchy created under */var/lib/zope*. This new user "zope" is a disabled user that is useful only for running the [Zope](#) service. [Zope](#) is now installed.

Both [Zope](#) and [Plone](#) require [Python](#); since all [FC3](#) packages were installed, this is not an issue.

To install [Plone](#) from source code, the commands are as follows (as root):

```
$ cd /root/zope
$ gzip -d Plone-2.0.5.tar.gz
$ tar xf Plone-2.0.5.tar
$ cd Plone-2.0.5
$ mv * /var/lib/zope/Products
$ chown -R zope:zope /var/lib/zope
```

[Plone](#) is now installed. To start up the [Zope/Plone](#) service, execute the following command (as root):

```
$ /etc/init.d/zope start
```

If [Zope](#) does not start correctly, there will be an error message³; the messages are generally self-explanatory.

Under [X Windows](#), open <http://localhost:8080> (using the default desktop web browser [Htmlview](#), for example). This will bring up the default [Zope](#) web page. This page will state that there are no valid users for this instance of [Zope](#). This does not preclude [Zope](#) from working correctly. However, it is necessary to create at least one valid [Zope](#) user in order to be able to access the [Zope](#) service. This can be done using [Zope](#)'s command line interface (CLI). The CLI is a program with its own command line, similar to the system shell, where specific key commands can be executed to perform [Zope](#)-related tasks. To start the CLI and add a user, run the following commands:

```
$ /var/lib/zope/zopectl
zopectl> stop
zopectl> adduser zope "hard_to_guess_password_goes_here"
zopectl> start
zopectl> quit
```

URL <http://localhost:8080/manage> will present a login window where the newly created user can log in to the [Zope](#) service. This can be seen in Figure 1.

³ It may also complain and print out some debugging information.

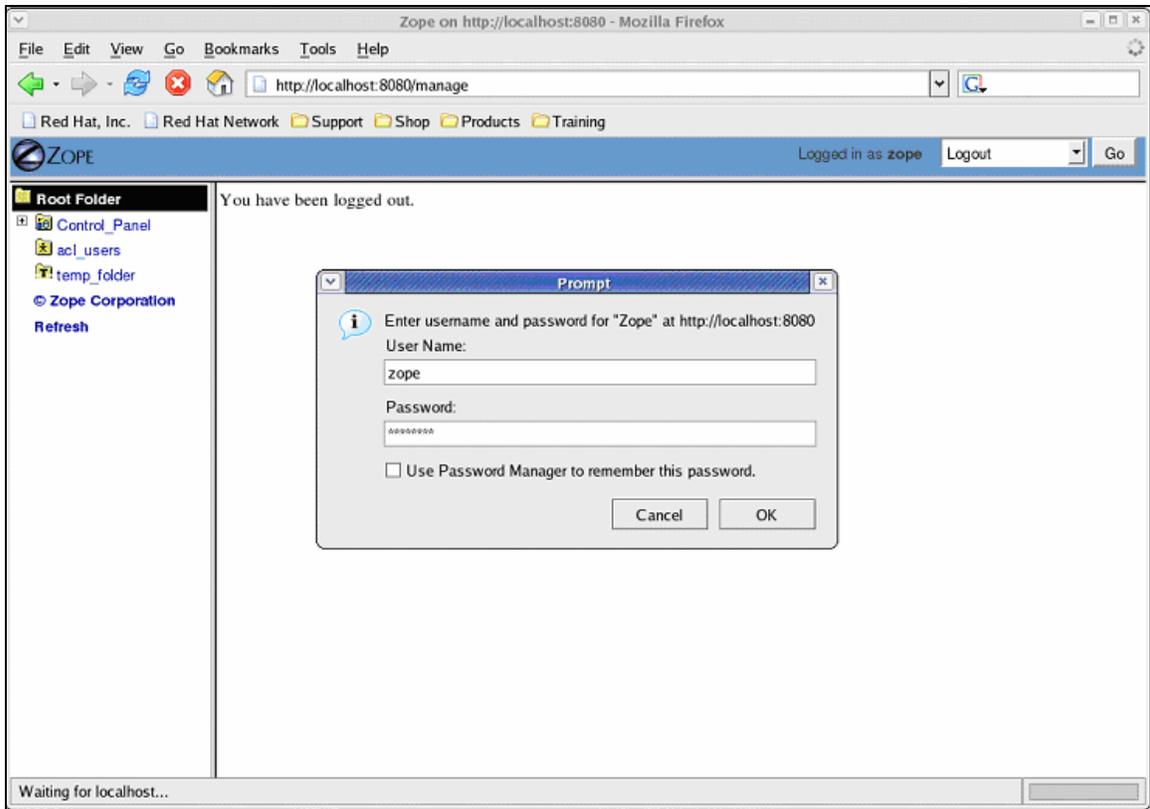


Figure 1. Logging in to [Zope](#)

Once logged in to [Zope](#), the user is presented with the [Zope Management Interface \(ZMI\)](#). This interface can be used to manage most of the different aspects and features of [Zope](#). This can be seen in Figure 2 where these options are apparent. No configurations are needed yet. Before that, it is necessary to compile and install the other components that were downloaded.

To install the [WV](#) package, use the following commands:

```
$ cd /root/zope
$ gzip -d wv-1.0.3.tar.gz
$ tar xf wv-1.0.3.tar
$ cd wv-1.0.3
$ ./configure
```

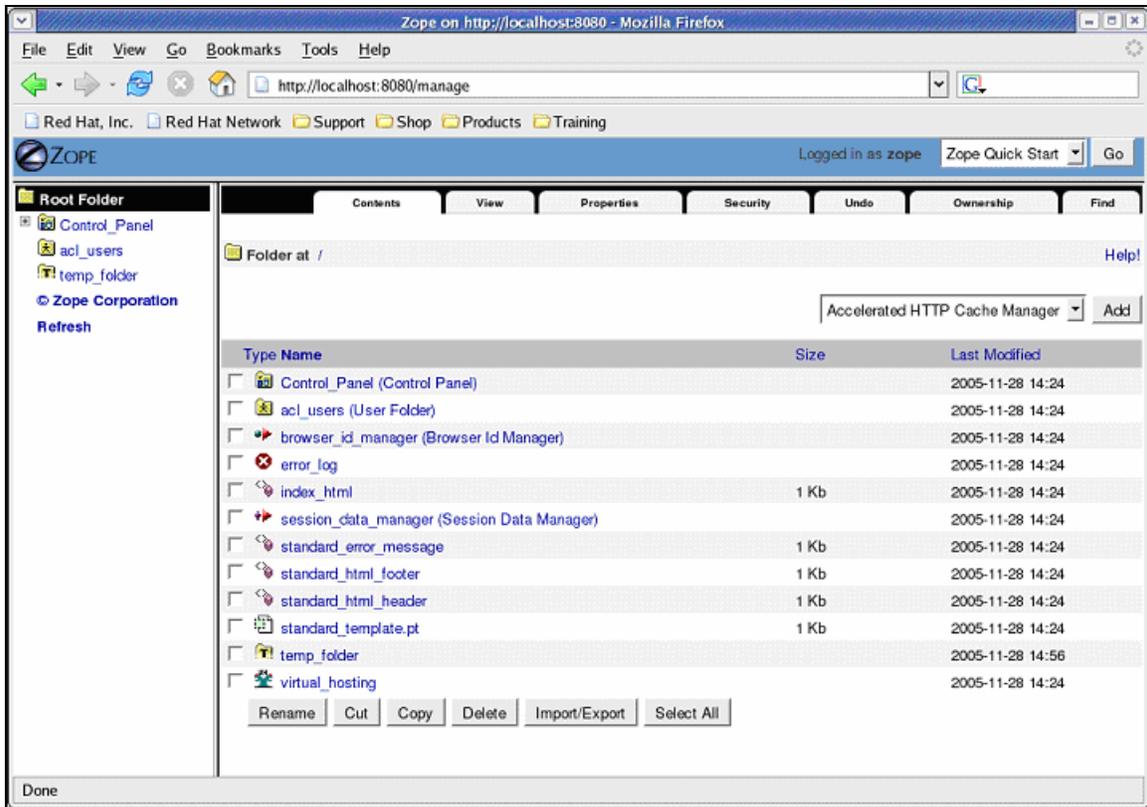


Figure 2. The [ZMI](#) and other configurable options

```
$ make
```

```
$ make check
```

```
$ make install
```

[WV](#) is now installed.

Next, install the package [TextIndexNG](#). For this, use the following commands:

```
$ cd /root/zope
```

```
$ gzip -d TextIndexNG-2.2.0b2.tar.gz
```

```
$ tar xf TextIndexNG-2.2.0b2.tar
```

```
$ cd TextIndexNG2
```

```
$ cd /usr/bin
```

```
$ ln -s python python2.2
```

```
$ cd /root/zope/TextIndexNG2
$ make clean
$ make perm
$ make build
$ make install
$ cd ..
$ mv TextIndexNG2 /var/lib/zope/Products
$ chown -R zope:zope /var/lib/zope
```

Finally, install the [Catdoc](#) package using the following commands:

```
$ cd /root/zope
$ gzip -d catdoc-0.94.tar.gz
$ tar xf catdoc-0.94.tar
$ cd catdoc-0.94
$ ./configure
$ make
$ make install
```

Once all packages and add-ons have been installed, the [Zope](#) service can be restarted. To verify that all the packages/add-ons are loaded and working correctly, the [Zope](#) service can be run with verbose debugging output enabled. This can be done as follows:

```
$ cd /var/lib/zope/bin
$ ./runzope &
```

The verbose output from starting [Zope/Plone](#) on the portal system can be found in Annex [A.1](#). This provides an example of what a [Zope/Plone](#) start-up should look like after all the packages have been installed.

To remove the various packages installed, simply delete them from the storage location found under */var/lib/zope*.

1.5 Creating the Plone site

To create a [Plone](#) site, go to <http://localhost:8080/manage> and log in to [Zope](#) using the “zope” user created in Section [1.4](#). A successful [Zope](#) login will provide access to the [ZMI](#) as shown in Figure 2.

Looking at Figure 2, on the far right hand side of the image is the *Add* button. Changing the selected “Accelerated HTTP Cache Manager” to “Plone Site” from the list box will create a new [Plone](#) site. Clicking the *Add* button, the browser displays a new page requiring information. Required fields, as well as sample data, are shown in Table 2.

Table 2. Values used for creating a new [Plone](#) site

Field	Value
Id	test2
Title	test2
Membership source	Create a new user folder in the portal
Description (optional)	This is a test site for documentation purposes

Once the information has been entered, clicking “Add Plone Site” will create the new site. This can be seen in Figure 3. For the purpose of this document, a test site named *test2* was created.

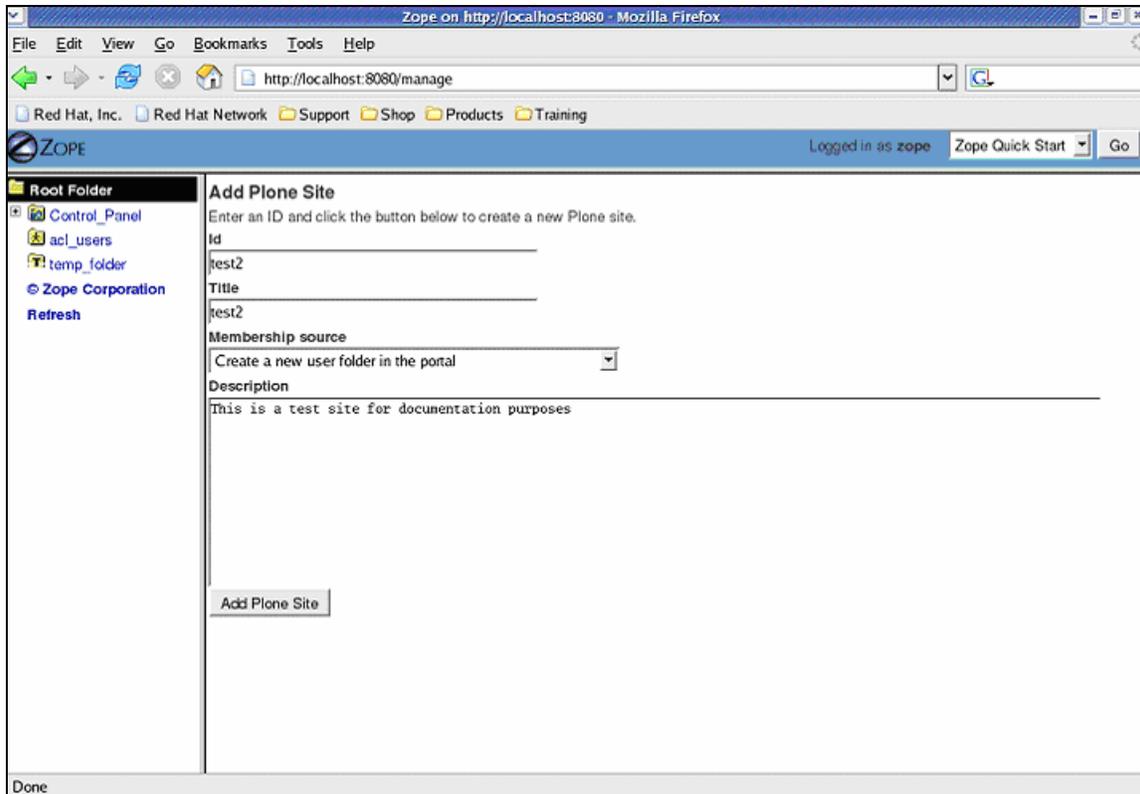


Figure 3. Fields and sample data required for creating a new [Plone](#) site

The new [Plone](#) site should now have been created; this part can be time consuming depending on the system's speed and available resources. Once complete, the new [Plone](#) site will be presented via the browser, as shown in Figure 4. From here, it can be completely reconfigured and modified according to the necessary requirements.

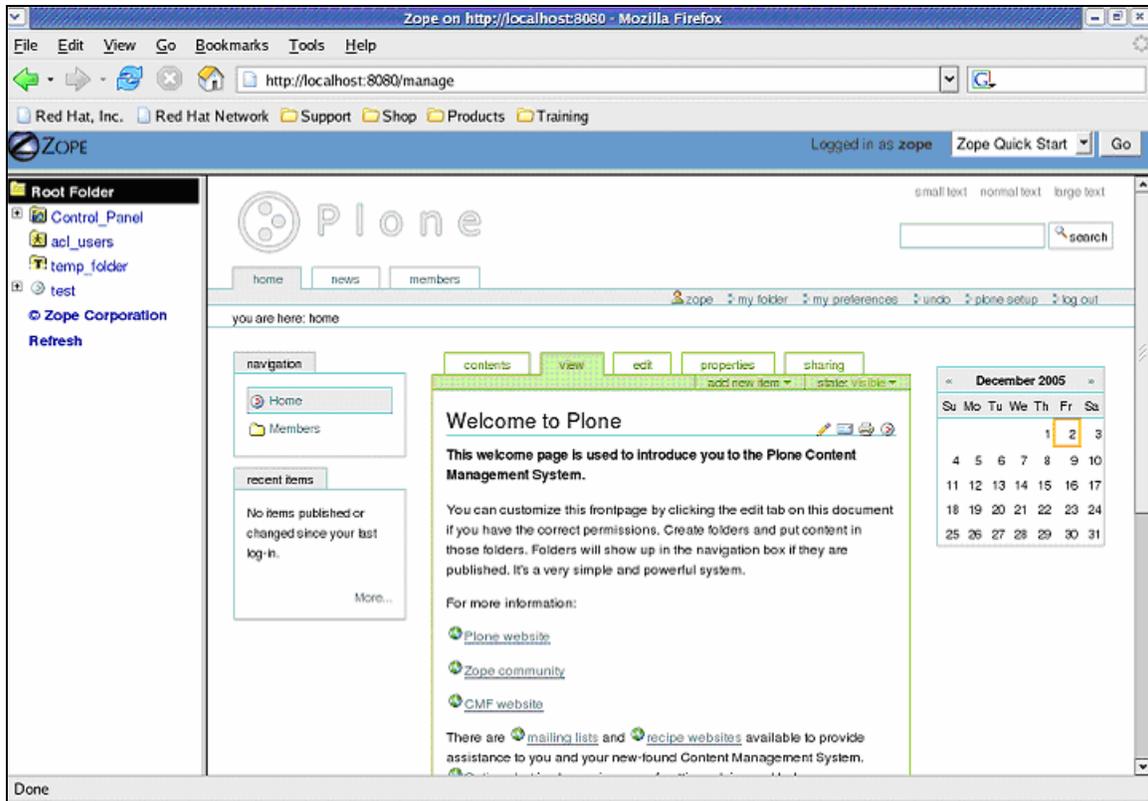


Figure 4. The newly-created [Plone](#) site

While configuring [Plone](#) can be complex, depending on the functionality required, what has been shown thus far is sufficient for anyone wishing to create his or her own [Plone](#) site. For those requiring more information, it is available from the product’s web site. At this point, the user can log out from [Zope](#) and close the web browser.

It is important to note that the user “zope” was allocated all the available rights and permissions at creation time (by default). In creating subsequent users, it is important to remember only to allocate the rights and permissions that are specifically needed by that user.

Reopening the web browser and pointing it to <http://localhost:8080/test2> will present the new [Plone](#) site that was just created and require a login (Figure 5). [Plone](#) is logged into the same way as the [ZMI](#).

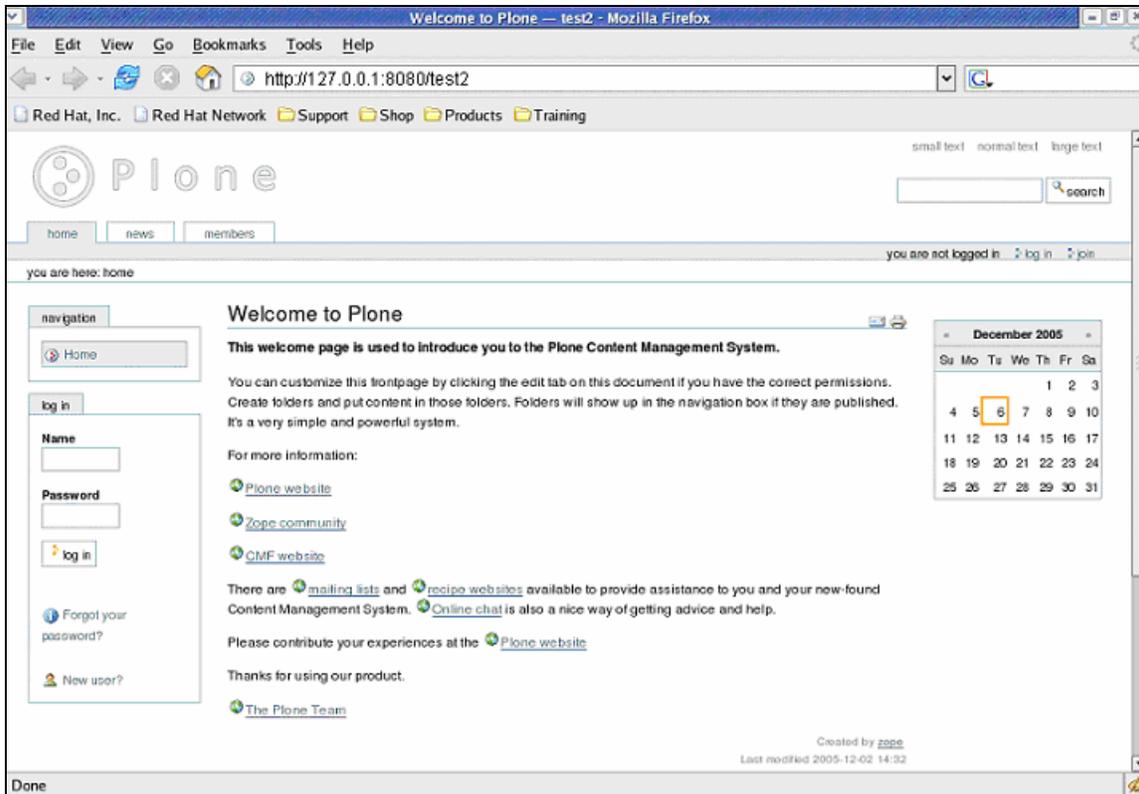


Figure 5. The new [Plone](#) site “test2”

1.6 Configuring WebDAV

[Zope](#) supports two methods for uploading files. They are WebDAV and FTP uploading. WebDAV is a protocol that provides a means to modify, delete, change, or create documents on remote systems. WebDAV is more complete as a document editing protocol than FTP. Thus, it is appropriate that, for a portal-based system, WebDAV be enabled rather than FTP. This is done by modifying the configuration file `/var/lib/zope/etc/zope.conf`. This file is short and easy to modify. The portal system’s WebDAV configuration is based on [1]. After modifications, with FTP disabled and WebDAV enabled, the file should appear as follows:

```
#<ftp-server>
# valid key is "address"
# address 8021
#</ftp-server>
<webdav-source-server>
# valid keys are "address" and "force-connection-close"
address 1980
```

```
force-connection-close off
</webdav-source-server>
```

Statements are commented out using the symbol #.

The [Zope](#) service must be restarted to reflect these changes.

1.7 Setting up the virtual host

Virtual hosting is used to hide the physical folder name(s) and to hide a web site's hierarchal structure. Because the portal system is to be used by [TTCP](#) counterparts, it was considered appropriate to implement virtual hosting to provide certain minimal web security features. Thus, data that is to be shared or displayed can be done so without the end-user knowing the basic structure or folder names. Virtual hosting takes one URL and converts it to another. It is also required for SSL (see Section [2.2](#)). Virtual hosting is done at the web server level; [Apache](#) provides all of the necessary modules for virtual hosting.

Before modifying [Apache](#), back up its configuration file (`/etc/httpd/conf/httpd.conf`) using the following commands:

```
$ cd /etc/httpd/conf
$ cp httpd.conf httpd.conf.backup
```

Several different fields in the file require modification. Using a text editor, the following items must be modified:

Step 1:

Find and modify the line:

```
ServerAdmin root@localhost
```

to:

```
ServerAdmin system_administrator@yoursite.com
```

Step 2:

Find and modify the line:

```
#ServerName new.host.name:80
```

to:

```
ServerName your portal's IP address
```

Step 1 changes the default e-mail address to that of the system administrator. This will cause administrative/error messages to be sent via e-mail. Step 2 states the IP address (or DNS hostname) of the system to use when creating URL redirections for the [Apache](#) web server. This feature is not compatible with DHCP-based addresses. The IP address can be used if a DNS entry

for portal system does not exist. If a DNS entry does exist, then use the DNS-based name for the system.

Based on [2], enabling virtual hosting requires that the following lines be appended to the file `/etc/httpd/conf/httpd.conf`:

Step 3:

```
<VirtualHost *>
    ServerName 143.146.253.7
    RewriteEngine on
    RewriteRule ^/(.*)
    http://143.146.253.7:8080/VirtualHostBase/http/143.146.253.7:80/
        VirtualHostRoot/$1 [L,P]
</VirtualHost>
```

[Apache](#) will also perform the same virtual hosting on the system's local loopback address. It is important to replace all instances of the portal system's IP address with one's own. Again, the line `ServerName` must be either the IP address or the DNS entry, depending on the availability of DNS.

In order to ascertain if a series of modifications will work when the [Apache](#) web server is restarted, simply test the configuration file using the following command:

```
$ /etc/init.d/httpd configtest
```

If there is no error output⁴, then the configuration file is valid and the [Apache](#) web server can be restarted with the following command:

```
$ /etc/init.d/httpd start
```

Going to <http://143.146.253.7/manage> or <http://143.146.253.7/test2>⁵, both the [ZMI](#) and [Plone](#) will be brought up, respectively. Note that it is no longer necessary to specify port **8080** anymore because the [Apache](#) web server now picks up all requests on port 80. This is shown in Figure 6. It can be said that virtual hosting helps to standardize web server access. In fact, specifying port **8080** will no longer work and the web page will not be accessible.

⁴ It may complain and print out some debugging information.

⁵ It is also possible to specify either "localhost" or IP address "127.0.0.1" instead of 143.146.253.7.

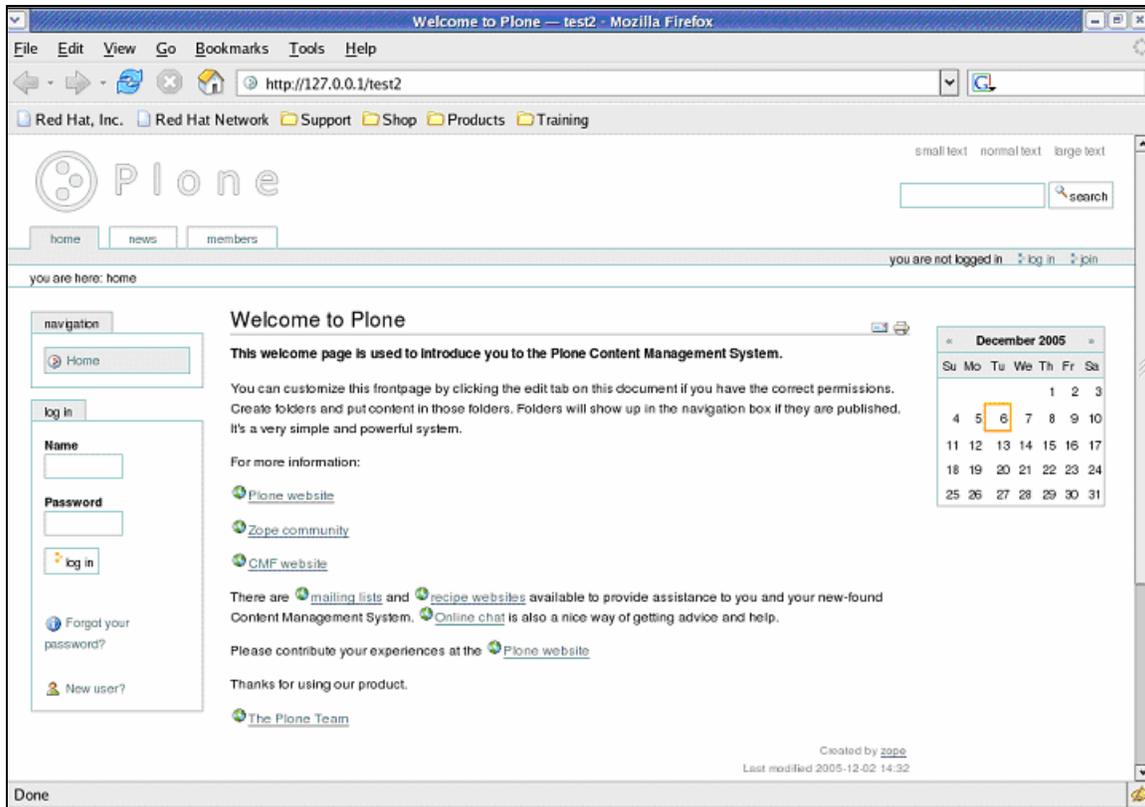


Figure 6. Example of virtual hosting without specifying port 8080 to access the [Plone](#) site

1.8 Securing the portal system

1.8.1 Disabling system services

It is important to disable all non-essential system and network services on the portal system. These services are generally found under both [Xinetd](#) (*/etc/xinetd.d*) and */etc/init.d*. The former is the Extended Internet Super Daemon that handles various services such as *Telnet*, *FTP*, *RSH*, etc. The latter is the storage location for most of the system services. These services can be enabled/disabled using two [Red Hat/FC3](#) specific tools, [Ntsysv](#) and [Serviceconf](#). The former is a command line based tool while the latter is an [X Windows](#) based tool. Their operation is simple and must be used on each concurrent system runlevel in order to set the services that will be run at start-up or upon initialization of a given runlevel.

The rule of thumb, particularly when a system such as the portal system is to be made accessible to the Internet via the sandbox, is to run only those services that are required. Thus, the system was set to come up to runlevel 3 upon start-up by modifying the file */etc/inittab*. All Xinetd services were disabled, as were all of the system and network services found under */etc/init.d*. The only services that were left running were: [Anacron](#), [Apache](#), [Atd](#), [Cron](#), [Network](#), [Postfix](#), [Sshd](#), [Syslog](#), [Sysstat](#), [Xinetd](#), and, of course, [Zope](#). Run *RPC*'s with the utmost care, as they are inherently very insecure.

When the first [Nessus](#) security scan was run, it was done with the default services running. However, the second scan was done with only the abovementioned services running (the report can be found in annexes [B.1](#) and [B.2](#)). The impact on the results in terms of vulnerabilities found was staggering. Thus, to reduce vulnerability-based issues, the disabling of non-essential services is paramount.

While disabling unused system services is always an important step, it cannot always be counted on for fixing security holes. The underlying operating system must be kept up to date. The importance of keeping a system up to date will be further emphasized in sections [1.8.2](#) and [1.8.3](#). While the portal system was built using [FC3](#), at this writing, versions that are more recent are available. It is highly recommended to always utilize a recent version of a distribution.

1.8.2 Configuring the security scanner

The main reason for installing and using a security and vulnerability assessment tool is to ascertain the level of attack-resistance that a given system has before it is connected to the sandbox. Corporate network operations will perform their own security assessment; however, their scan does not ordinarily reveal how to fix a given problem. The open source security assessment tool [Nessus](#) is just as powerful as its commercial counterparts and usually does provide meaningful information on how to fix a given security vulnerability. [Nessus](#) must be downloaded and compiled. Before that can occur, it is critical that a system update be performed on the portal system. [FC3](#) comes equipped with the necessary software to perform this task: [up2date](#). Updating will reduce the number of critical security issues found by [Nessus](#).

[Nessus](#), after downloading, should be copied to the portal system under `/root/zope`. At the time of writing, [Nessus](#) is at version 2.2.6 and comes in four components: plugins; core components, core libraries, and scanner libraries. The files that were downloaded are:

```
nessus-core-2[1].2.6.tar.gz
nessus-libraries-2[1].2.6.tar.gz
nessus-plugins-2[1].2.6.tar.gz
libnasl-2[1].2.6.tar.gz
```

The tools are compiled and installed with the following commands, *in this order*:

```
$ cd /root/zope
$ mkdir nessus
$ mv libnasl* nessus
$ mv nessus-* nessus
$ cd nessus
$ gzip -d *
```

```
$ tar xf libnasl-2\[1\].2.6.tar
$ tar xf nessus-core-2\[1\].2.6.tar
$ tar xf nessus-libraries-2\[1\].2.6.tar
$ tar xf nessus-plugins-2\[1\].2.6.tar
$ cd nessus-libraries
$ ./configure
$ make
$ make install
```

Modify the file */etc/ld.so.conf* by appending the following entry to it:

```
    /usr/local/lib
$ ldconfig
```

Modify the file */etc/bashrc* by appending the following entries to it:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
PATH=$PATH:/usr/local/bin:/usr/local/sbin
export PATH
$ source /etc/bashrc
$ cd ../libnasl
$ ./configure
$ make
$ make install
$ cd ../nessus-core
$ ./configure
$ make
$ make install
$ cd ../nessus-plugins
```

```
$ ./configure
$ make
$ make install
```

If all goes well, [Nessus](#) is now successfully installed. A description of configuring and running the security tool is provided below.

1.8.3 Running the security scanner

The [Nessus](#) tools are command-line based and require root privilege to be run. Before running [Nessus](#), several steps must be performed. It is necessary to create the security certificate, which is similar to a SSL certificate. It too is used to secure the network stream for remote usage and authentication. To create the certificate, run the following command:

```
$ nessus-mkcert
```

The command will ask for certain information, an example of which is shown in Table 3.

Table 3. Fields and values for creating [Nessus](#) certificate

Field	Value Entered
CA certificate life time in days [1460]	accept default by pressing Enter key
Server certificate lifetime in days [365]	accept default by pressing Enter key
Enter Country Code	Enter in CA for Canada
Provide the name of your province/state	Quebec
Provide your organization	DRDC Valcartier

Once the certificate is created, the security scanner can be started using the following command:

```
$ nessusd &
```

This runs the [Nessus](#) daemon that will load all of the 10,000+ plugins. Once complete, it is necessary to create a [Nessus](#) user using the following command:

```
$ nessus-adduser
```

The username “nessus” is an appropriate choice for a [Nessus](#) user. The program will query for various pieces of information such as user name and password authentication. The security scanner must be started up under [X Windows](#). This is done by running the following command:

```
$    nessus &
```

This will bring up the [Nessus](#) client interface. The user must log in to the interface using the “nessus” user and its password.

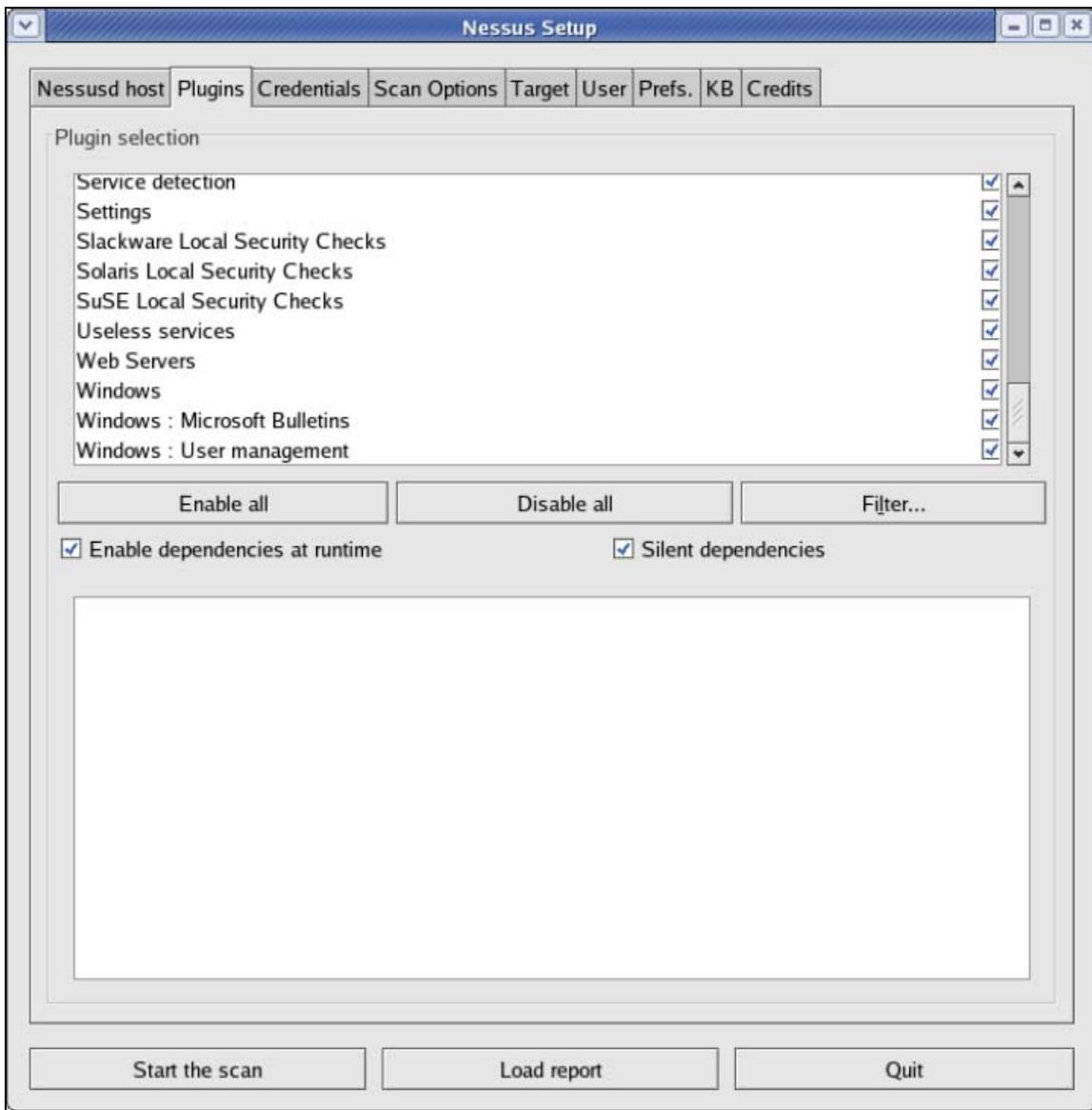


Figure 7. Example of user-configurable features via the [Nessus](#) client interface

[Nessus](#) is highly configurable and its scans can be customized by modifying the various groupings of options found under the various tabs. This is shown in Figure 7. Once the

appropriate scanning options have been chosen, it is then possible to proceed with the scan. Both remote and local systems can be scanned. For the needs of the portal system, the local system will be scanned since [Nessus](#) is already running local on it. The scan can take several hours to complete. Time will be largely dependent on the speed of the system. If scanning a remote site, disable any firewall on either system.

[Nessus](#) can cause scanned systems to crash. If this happens, it will be necessary to adjust the scanning and testing options.

A [Nessus](#) generated report can be very long. The report in Annex [B.1](#) and [B.2](#) is more than a hundred pages in length. The included report demonstrates a security scan that was performed before a system update was done. The importance of performing a system update before running the security scan cannot be overstressed. After performing the system update, but before disabling unneeded system services (see Section [1.8.1](#)), only about 15 pages of security issues were found instead of more than a hundred. This made dealing with the issues more manageable. Moreover, after disabling all of the unneeded services and running the scanner a third and final time, only three security warnings were found that, after reading them, could be safely ignored.

1.9 Wrap up

At this point, it is appropriate to have corporate network operations perform a security and vulnerability assessment of the portal system. However, most if not all of the major security issues should already have been found using [Nessus](#) and fixed by both performing the system update and disabling unneeded system services. Once any major issues have been mitigated, the system can then be connected to the sandbox. This must be done with the help of local technical support services. Once connected, the system must be powered on and network connectivity tests must be performed. It is possible that certain network-based issues will have to be corrected such as a two-way DNS or one-way mail redirection (Section [2.1](#)).

Again, the importance of utilizing a recent distribution for portal deployment is paramount. This cannot be overstated, as seen in Section [1.9](#). There, it is obvious to see how using a recent or updated operating system reduces the complexities of resolving too many security issues that quickly become a burden.

2. Optional component implementation

2.1 Implementing mail redirection

The mail redirection option should only be used if it is not possible to send e-mails directly from the portal system. Sandbox-like systems will probably block outgoing mail transfers but may allow for transfers to specific internal mail systems. Essentially, mail redirection can be likened to a mail bounce, where e-mail is sent from the originator to an alternate system for delivery. Thus, depending on specific network configurations, operational policies, and procedures, this section may or may not be important.

It is useful for e-mails to be sent because users can be alerted to such as account creation and modification or system issues. Under [Linux](#), mail redirection is normally done using the [UNIX Sendmail](#) program. However, [Sendmail](#) is large, complex, and cumbersome to use and configure. Thus another open source tool can be used, [Postfix](#). Much easier to use and configure, it does use [Sendmail](#) as its backend anyway.

Based on [\[3\]](#), it is necessary to modify [Postfix](#)'s configuration file (*/etc/postfix/main.cf*) as follows:

Find and modify the line:

```
relayhost =
```

to:

```
relayhost = mail_server_name
```

or to:

```
relayhost = mail_server_IP_address
```

[Postfix](#), like [Sendmail](#), generates warning messages and debug information that can be found in the file */var/log/maillog*.

2.2 Setting up SSL

2.2.1 Introduction

SSL is used to secure communications between a web server and a remote client. Because the portal system is used by [TTCP](#) counterparts, it was requested that SSL be enabled to secure the network stream against electronic eavesdropping.

SSL uses certificates, which come in two forms: signed and unsigned. Signed certificates can either be self-signed (signed by the organization that created them) or signed by an authorized signing authority such as [VeriSign](#).

Different circumstances will call for different types of certificates. However, because international counterparts will use the web services provided by the portal system and security is prerequisite, only self-signed certificates will be used. The procedures listed below are valid for creating self-signed certificates, and there is more than one way to do this. The commands in the following sections are based on an amalgamation of information found in various references and sources.

2.2.2 Creating a signed SSL key/certificate

Based on [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#) [\[13\]](#), to create a signed key/certificate, perform the following operations. Before the signed certificate can be created, create the **key** by running the following commands:

```
$ cd /root
```

```
$ openssl genrsa -des3 2048 > /etc/httpd/conf/ssl.key/server.key
```

This command will generate a [DES3](#)-based 2048-bit [RSA](#) key. This command **will require a passphrase** to be entered and then re-entered. It is important that the passphrase be put in a safe place so that it is not forgotten because it will be needed shortly.

The next step is to create the **self-signed certificate**, using the following command:

```
$ openssl req -new -key /etc/httpd/conf/ssl.key/server.key -x509 -nodes -sha1  
-days 730 -out /etc/httpd/conf/ssl.crt/server.crt
```

This command creates a self-signed certificate that is valid for two years from the date of creation. When the certificate expires, simply create a new one and replace the old one. The passphrase used in the first *openssl* command must now be entered for the second *openssl* command in order to process the key.

After running the second *openssl* command, certain pieces of information must be provided. An example of this is shown here with sample responses in bold:

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]: **CA**

State or Province Name (full name) [Berkshire]: **QUEBEC**

Locality Name (eg, city) [Newbury]: **VALCARTIER**
Organization Name (eg, company) [My Company Ltd]: **DRDC**
Organizational Unit Name (eg, section) []: **SI**
Common Name (eg, your name or your server's hostname) []: **PORTAL**
Email Address []: **firstname.lastname@drdc-rddc.gc.ca**

The certificate request is now created and stored in the correct location. The certificate is now ready to be used directly by [Apache](#).

To verify and examine the certificate, the following two commands could be used:

```
$ openssl x509 -fingerprint -text < /etc/httpd/conf/ssl.crt/server.crt | more
```

or

```
$ openssl x509 -fingerprint -text < /etc/httpd/conf/ssl.crt/server.crt >  
/etc/httpd/conf/ssl.crt/host.info
```

The first command can be used to pipe the output to the console and the second to store the output in a file.

2.2.3 Configuring SSL virtual hosting

In order to configure SSL virtual hosting, changes need to be made to the virtual hosting options appended to the file `/etc/httpd/conf/httpd.conf` in Section [1.7](#). To use SSL, the following changes must supersede any of the changes made in Section [1.7](#). According to [\[7\]](#) [\[8\]](#) [\[9\]](#) [\[10\]](#) [\[11\]](#) [\[12\]](#) [\[13\]](#), the following changes must be made to the file `/etc/httpd/conf/httpd.conf`:

```
<IfModule mod_ssl.c>  
<VirtualHost *:443>  
    ServerName 143.146.253.7  
    SSLEngine on  
    SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt  
    SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key  
    SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown  
    RewriteEngine on  
    RewriteRule ^(login_form)$ https:// 143.146.253.7/$1/$2 [R,noescape]  
    RewriteRule ^/(.*)  
    http://143.146.253.7:8080/VirtualHostBase/https/143.146.253.7:443/VirtualHostRoot/$1 [P,L]  
</VirtualHost>
```

</IfModule>

Note the entries *SSLCertificateFile* and *SSLCertificateKeyFile*; both entries point to the correct certificate and key file. Once the changes have been made, both [Apache](#) and [Zope](#) will have to be restarted. Once restarted, all the services will be accessible via the HTTPS connection. This includes connections to both <https://143.146.253.7/test2> and <https://143.146.253.7/manage>.

It is also important that the line *ServerName* is the same as the one defined in Section [1.7](#). Furthermore, the *ServerName* entry is dependent on the availability of the DNS entry for the portal system. If the DNS entry is available, then the DNS host name is inserted here as well as for the *ServerName* line configured in Section [1.7](#). Otherwise, the IP address of the portal system is to be used.

A full copy of the modified *httpd.conf* can be found in Annex [A.2](#). Furthermore, changes must be made to the file */etc/httpd/conf.d/ssl.conf*. Its content can be found in Annex [A.3](#).

If [Apache](#) is started up at boot time then it will be necessary to enter the password at that time; otherwise, SSL will not be available.

Once SSL is operational via [Apache](#), it will no longer be possible to access the portal system via the conventional HTTP port 80 or via the default [Zope/Plone](#) port 8080. Only port 443 will be accessible.

Pointing a web browser to <https://143.146.253.7/test2> or <https://143.146.253.7/manage> will present a popup window stating that the certificate has been signed by an unknown authority and query for continuation. This popup is shown in Figure 8.

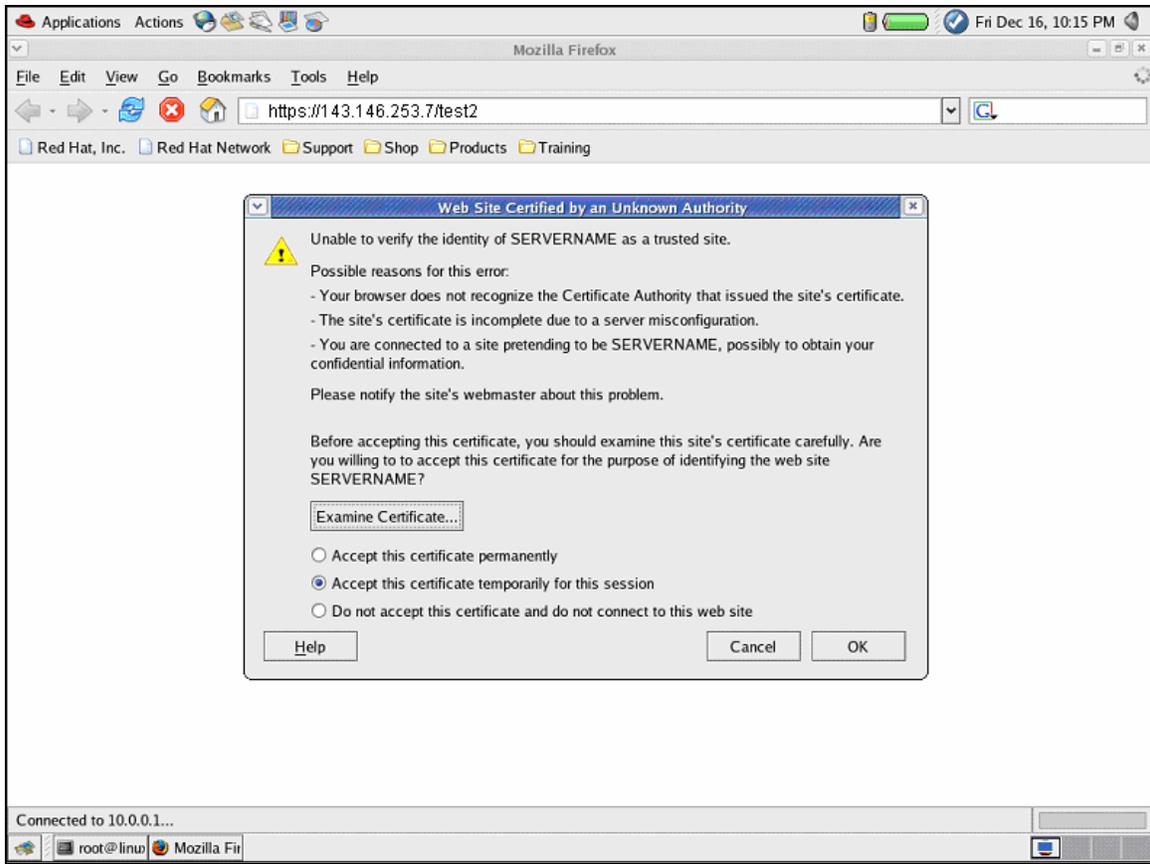


Figure 8. Accepting a certificate signed by an unknown authority

Clicking on the button “Examine Certificate” displays the details of the certificate. A message should be sent to all offsite counterparts instructing them of the new certificate and how to verify that the authenticity of the signed certificate via their browser.

2.2.4 Miscellaneous

There are many ways to create a self-signed certificate. Some methods require running the *sign.sh* program. However, this program requires that certain prerequisites exist such as configured SSL configuration files, *ca.config* and *openssl.cnf*. These files are quite difficult to configure.

Other methods will require the use of various “makefiles” provided with [OpenSSL](#). Unfortunately, these files themselves do not always work and often require both *ca.config* and *openssl.cnf* to exist and be correctly configured.

Thus, what has been shown is not the only method, or necessarily the best method; however, it works and is quick and easy to use and understand. Furthermore, it does not require much configuration or tweaking.

3. Conclusion

It has been demonstrated, using a systematic approach, how to build, install, configure, and rapidly deploy a portal-based CMS system based on open source products [Linux](#), [Zope](#), and [Plone](#).

The entire system, starting with the installation and basic configuration of Linux can be done in several hours. The compilation and installation of [Zope](#) and [Plone](#) should only take two hours at most, even on relatively slow systems. The longest part is the update process. Depending on the version of [Fedora Core Linux](#), including the number of packages needed for the update process, as well as the speed of the download connection, it can take between 2 hours to a little over a day. Creation and installation of the SSL key/certificate, following the provided instructions, are a relatively short endeavour.

The most complex task to perform is the security audit. This can be not only time consuming but the tasks required to remedy the various security issues found can be difficult. Fortunately, at least for [Linux](#) and other [UNIX](#)-based systems, [Nessus](#) is very verbose about the issues found as well as how to fix them. Generally, an update of the operating system and disabling of unneeded system services will result in far fewer issues being found by [Nessus](#). Furthermore, security issues vary in severity; warnings can often be ignored after reading through the information provided by [Nessus](#) and concluding that it is safe to do so. However, the major security flaws and vulnerabilities have to be remedied.

Fixing security issues, whether major or minor in importance, will have to be done on a case-by-case basis. Once [Nessus](#) delivers a clean bill of health, the probability of corporate network operations finding a problem with the system is very low.

Once the security-related aspects of the installation and configuration are complete, the system can then be allowed access to the Internet where the various [TTCP](#) members can access the portal and begin working with the system.

While some portions of the process may seem longer than others to complete, the whole process, from start to finish, should require less than 3 working days of effort. Do not worry; most of it does not require standing in front of the computer! If certain aspects are left out such as mail redirection or SSL, time will be saved. Implement only what is needed. As mentioned, most of the time will be spent fixing the major security issues and in the update process. Therefore, in order to minimize the impact of both these aspects, a more recent distribution should be chosen. While [Fedora Core 3](#) was chosen because it was the current [Fedora Core](#) distribution, today it is very much out of date and a newer one such as [Fedora Core 5](#) should be used in its place.

References

- [1] Stain. Using WebDAV. Plone Foundation. Howto. February 2006.
<http://plone.org/documentation/how-to/webdav>.
- [2] Amos Latteier, et al. The Zope Book, Ch. 19: Virtual Hosting Services. Revision 2.6. Zope Community. Book. http://www.zope.org/Documentation/Books/ZopeBook/2_6Edition/VirtualHosting.stx.
- [3] Venema, Wieste. Postfix Configuration Parameters. Postfix. Configuration Article.
<http://www.postfix.org/postconf.5.html>.
- [4] Sigle, Richard. Building a Secure RedHat Apache Server HOWTO. Revision 0.1. The Linux Documentation Project. Howto. June 2001. <http://www.tldp.org/HOWTO/SSL-RedHat-HOWTO.html>.
- [5] Zope Community. SSL Certificate. Zope Community. Web article.
<http://www.zope.org/Members/vernier/Debian/SSLcertificate>.
- [6] Raible, Matt. The Apache + SSL HOWTO. Version 1.6.8. Raible's Wiki. Howto. September 2002. <http://raibledesigns.com/wiki/Wiki.jsp?page=ApacheSSL>.
- [7] Runyan, Alan. Setting Up Plone behind Apache with SSL. Zope Community. Web article. August 2006. <http://plone.org/documentation/how-to/apache-ssl>.
- [8] Red Hat. Red Hat Linux 9: Red Hat Linux Configuration Guide. Red Hat. User manual. 2003. <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/pdf/rhl-cg-en-9.pdf>.
- [9] Kalupson, Kevin J. Zope with Apache and SSL. Pennsylvania State University. Web article. August 2005. http://zope.psu.edu/tutorials/zopetut/zope_apache_ssl.
- [10] Doyle, Allan. Plone via HTTPS. EOGEO. Web Article. February 2006.
<http://www.eogeo.org/Members/adoyale/ad-snippets/plone-via-mod-ssl>.
- [11] Cooper, Cameron. Content Management With Plone: An in-depth and comprehensive guide to the Plone content management system. ISBN 1904811027. Packt Publishing. Book. November 2004. http://plonebook.packtpub.com/1027_14_PreviewChapter.pdf.
- [12] Ford, Andrew. Apache Pocket Reference. First Edition. ISBN 1-56592-706-0. O'Reilly & Associates. Book. June 2000.
- [13] Mourani, Gerhard. Securing and Optimizing Linux: RedHat Edition – A Hands on Guide. OpenDocs LLC and XML Source. Online Book. 2000.
<http://www.faqs.org/docs/securing/>.

Annex A System configurations, tests, and outputs

A.1 Verbose Zope start-up output detailing optional tools and features

In the following, the correct output of a start-up of the [Zope](#) service third-party products can be seen. Only the [pptHtml](#) service is not working because the program could not be found for installation.

2005-11-28T19:02:30 INFO(0) ZServer HTTP server started at Mon Nov 28 19:02:30 2005

 Hostname: Zope-server

 Port: 8080

2005-11-28T19:02:30 INFO(0) ZServer FTP server started at Mon Nov 28 19:02:30 2005

 Hostname: Zope-server

 Port: 8021

2005-11-28T19:02:30 INFO(0) Zope Set effective user to "zope"

2005-11-28T19:02:38 INFO(0) IngeniWeb

NOTICE global_symbols.py:20:Mon Nov 28 19:02:38 2005: 'Starting /var/lib/zope/Products/GroupUserFolder at 4 debug level'

2005-11-28T19:02:38 INFO(0) PlacelessTranslationService Applying patch

*** Patching ZPublisher.Publish with the get_request patch! ***

2005-11-28T19:02:40 DEBUG(-200) FileStorage create storage /var/lib/zope/var/Data.fs

2005-11-28T19:02:41 DEBUG(-200) TemporaryStorage create storage temporary storage for sessioning

2005-11-28T19:02:41 BLATHER(-100) ZODB Committing subtransaction of size 6198

2005-11-28T19:02:41 INFO(0) Archetypes
Products/Archetypes/content_driver/MSWord.py[20]:?

Failed to import the OpenOffice PyUNO content converter.

Remind me to write a doc on how to set this up as its a better
converter than wvWare and in some cases even MS Word

2005-11-28T19:02:49 INFO(0) PlacelessTranslationService Initialized:

['archetypes-sv.po', 'archetypes-bg.po', 'archetypes-pt-br.po'] from
/var/lib/zope/Products/Archetypes/i18n

2005-11-28T19:03:16 INFO(0) PlacelessTranslationService Initialized:

['plone-ko.po', 'plone-sv.po', 'plone-hr.po', 'plone-da.po', 'plone-es-ar.po', 'plone-fr.po', 'plone-es-
es.po', 'plone-ja.po', 'plone-es.po', 'plone-el.po', 'plone-en.po', 'plone-eo.po', 'plone-bg.po', 'plone-
ca.po', 'plone-he.po', 'plone-de.po', 'plone-pt-br.po', 'plone-zh-tw.po', 'plone-pt.po', 'plone-ro.po',
'plone-zh.po', 'plone-af.po', 'plone-no.po', 'plone-cs.po', 'plone-eu.po', 'plone-fa.po', 'plone-tr.po',
'plone-hy.po', 'plone-ru.po', 'plone-ar.po', 'plone-zh-cn.po', 'plone-nn.po', 'plone-uk.po', 'plone-
hu.po', 'plone-zh-hk.po', 'plone-fi.po', 'plone-nl.po', 'plone-lt.po', 'plone-pl.po', 'plone-it.po', 'plone-
ka.po', 'plone-et.po'] from /var/lib/zope/Products/CMFPlone/i18n

2005-11-28T19:03:16 INFO(0) PlacelessTranslationService Initialized:

['pts-de.po', 'pts-pt-br.po'] from /var/lib/zope/Products/PlacelessTranslationService/i18n

2005-11-28T19:03:16 INFO(0) PlacelessTranslationService Initialized:

['ploneerrorreporting-pt-br.po'] from /var/lib/zope/Products/PloneErrorReporting/i18n

2005-11-28T19:03:18 INFO(0) textindexng Converter "doc" for application/msword registered

2005-11-28T19:03:18 INFO(0) textindexng Converter "doc" for application/ms-word registered

2005-11-28T19:03:19 INFO(0) textindexng Converter "doc" for application/vnd.ms-word
registered

2005-11-28T19:03:19 INFO(0) textindexng Converter "ps" for application/postscript registered

2005-11-28T19:03:19 INFO(0) textindexng Converter "html" for text/html registered

2005-11-28T19:03:19 INFO(0) textindexng Converter "ooffice" for application/vnd.sun.xml.writer registered

which: no pptHtml in

(/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin)

2005-11-28T19:03:20 PROBLEM(100) textindexng Converter "ppt" not registered because executable "pptHtml" could not be found

2005-11-28T19:03:20 INFO(0) textindexng Converter "sgml" for text/sgml registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "sgml" for text/xml registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "xls" for application/msexcel registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "xls" for application/ms-excel registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "xls" for application/vnd.ms-excel registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "pdf" for application/pdf registered

2005-11-28T19:03:20 INFO(0) textindexng Converter "null" for text/plain registered

2005-11-28T19:03:21 BLATHER(-100) Z2 Installed sighandler for SIGTERM

2005-11-28T19:03:21 BLATHER(-100) Z2 Installed sighandler for SIGINT

2005-11-28T19:03:21 BLATHER(-100) Z2 Installed sighandler for SIGHUP

2005-11-28T19:03:21 BLATHER(-100) Z2 Installed sighandler for SIGUSR2

2005-11-28T19:03:21 INFO(0) Zope Ready to handle requests

A.2 File contents of httpd.conf

The full contents of the final version of the file */etc/httpd/conf/httpd.conf* are as follows:

```
ServerTokens OS
ServerRoot "/etc/httpd"
PidFile run/httpd.pid
Timeout 120
KeepAlive Off
MaxKeepAliveRequests 100
KeepAliveTimeout 15
<IfModule prefork.c>
StartServers      8
MinSpareServers   5
MaxSpareServers   20
ServerLimit       256
MaxClients        256
MaxRequestsPerChild 4000
</IfModule>
<IfModule worker.c>
StartServers      2
MaxClients        150
MinSpareThreads   25
MaxSpareThreads   75
ThreadsPerChild   25
MaxRequestsPerChild 0
</IfModule>
Listen 80
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
LoadModule auth_anon_module modules/mod_auth_anon.so
LoadModule auth_dbm_module modules/mod_auth_dbm.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule ldap_module modules/mod_ldap.so
```

LoadModule auth_ldap_module modules/mod_auth_ldap.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule cern_meta_module modules/mod_cern_meta.so
LoadModule expires_module modules/mod_expires.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule headers_module modules/mod_headers.so
LoadModule usertrack_module modules/mod_usertrack.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule mime_module modules/mod_mime.so
LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule asis_module modules/mod_asis.so
LoadModule info_module modules/mod_info.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule dir_module modules/mod_dir.so
LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
LoadModule speling_module modules/mod_speling.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule cache_module modules/mod_cache.so
LoadModule suexec_module modules/mod_suexec.so

```
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule file_cache_module modules/mod_file_cache.so
LoadModule mem_cache_module modules/mod_mem_cache.so
LoadModule cgi_module modules/mod_cgi.so
Include conf.d/*.conf
User apache
Group apache
ServerName 143.146.254.7
ServerAdmin firstname.lastname@drdc-rddc.gc.ca
UseCanonicalName Off
DocumentRoot "/var/www/html"
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
<Directory "/var/www/html">
    Options Indexes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
<IfModule mod_userdir.c>
    UserDir disable
</IfModule>
DirectoryIndex index.html index.html.var
AccessFileName .htaccess
<Files ~ "\.ht">
    Order allow,deny
    Deny from all
</Files>
TypesConfig /etc/mime.types
DefaultType text/plain
<IfModule mod_mime_magic.c>
```

```

MIMEMagicFile conf/magic
</IfModule>
HostnameLookups Off
ErrorLog logs/error_log
LogLevel warn
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
CustomLog logs/access_log combined
ServerSignature On
Alias /icons/ "/var/www/icons/"
<Directory "/var/www/icons">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
<IfModule mod_dav_fs.c>
    # Location of the WebDAV lock database.
    DAVLockDB /var/lib/dav/lockdb
</IfModule>
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
IndexOptions FancyIndexing VersionSort NameWidth=*
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
AddIconByType (TXT,/icons/text.gif) text/*

```

AddIconByType (IMG,/icons/image2.gif) image/*
 AddIconByType (SND,/icons/sound2.gif) audio/*
 AddIconByType (VID,/icons/movie.gif) video/*
 AddIcon /icons/binary.gif .bin .exe
 AddIcon /icons/binhex.gif .hqx
 AddIcon /icons/tar.gif .tar
 AddIcon /icons/world2.gif .wrl .wrl.gz .vrm .vrm .iv
 AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
 AddIcon /icons/a.gif .ps .ai .eps
 AddIcon /icons/layout.gif .html .shtml .htm .pdf
 AddIcon /icons/text.gif .txt
 AddIcon /icons/c.gif .c
 AddIcon /icons/p.gif .pl .py
 AddIcon /icons/f.gif .for
 AddIcon /icons/dvi.gif .dvi
 AddIcon /icons/uuencoded.gif .uu
 AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
 AddIcon /icons/tex.gif .tex
 AddIcon /icons/bomb.gif core
 AddIcon /icons/back.gif ..
 AddIcon /icons/hand.right.gif README
 AddIcon /icons/folder.gif ^^DIRECTORY^^
 AddIcon /icons/blank.gif ^^BLANKICON^^
 DefaultIcon /icons/unknown.gif
 ReadmeName README.html
 HeaderName HEADER.html
 IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
 AddLanguage ca .ca
 AddLanguage cs .cz .cs
 AddLanguage da .dk
 AddLanguage de .de
 AddLanguage el .el
 AddLanguage en .en

AddLanguage eo .eo
AddLanguage es .es
AddLanguage et .et
AddLanguage fr .fr
AddLanguage he .he
AddLanguage hr .hr
AddLanguage it .it
AddLanguage ja .ja
AddLanguage ko .ko
AddLanguage ltz .ltz
AddLanguage nl .nl
AddLanguage nn .nn
AddLanguage no .no
AddLanguage pl .po
AddLanguage pt .pt
AddLanguage pt-BR .pt-br
AddLanguage ru .ru
AddLanguage sv .sv
AddLanguage zh-CN .zh-cn
AddLanguage zh-TW .zh-tw
LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no pl pt pt-BR ru sv
zh-CN zh-TW
ForceLanguagePriority Prefer Fallback
AddDefaultCharset UTF-8
AddCharset ISO-8859-1 .iso8859-1 .latin1
AddCharset ISO-8859-2 .iso8859-2 .latin2 .cen
AddCharset ISO-8859-3 .iso8859-3 .latin3
AddCharset ISO-8859-4 .iso8859-4 .latin4
AddCharset ISO-8859-5 .iso8859-5 .latin5 .cyr .iso-ru
AddCharset ISO-8859-6 .iso8859-6 .latin6 .arb
AddCharset ISO-8859-7 .iso8859-7 .latin7 .grk
AddCharset ISO-8859-8 .iso8859-8 .latin8 .heb
AddCharset ISO-8859-9 .iso8859-9 .latin9 .trk

```

AddCharset ISO-2022-JP .iso2022-jp .jis
AddCharset ISO-2022-KR .iso2022-kr .kis
AddCharset ISO-2022-CN .iso2022-cn .cis
AddCharset Big5 .Big5 .big5
AddCharset WINDOWS-1251 .cp-1251 .win-1251
AddCharset CP866 .cp866
AddCharset KOI8-r .koi8-r .koi8-ru
AddCharset KOI8-ru .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8 .utf8
AddCharset GB2312 .gb2312 .gb
AddCharset utf-7 .utf7
AddCharset utf-8 .utf8
AddCharset big5 .big5 .b5
AddCharset EUC-TW .euc-tw
AddCharset EUC-JP .euc-jp
AddCharset EUC-KR .euc-kr
AddCharset shift_jis .sjis
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddHandler imap-file map
AddHandler type-map var
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
Alias /error/ "/var/www/error/"
<IfModule mod_negotiation.c>
<IfModule mod_include.c>
  <Directory "/var/www/error">
    AllowOverride None
    Options IncludesNoExec
    AddOutputFilter Includes html
    AddHandler type-map var

```

```

    Order allow,deny
    Allow from all
    LanguagePriority en es de fr
    ForceLanguagePriority Prefer Fallback
</Directory>
</IfModule>
</IfModule>
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\0" force-response-1.0
BrowserMatch "Java/1\0" force-response-1.0
BrowserMatch "JDK/1\0" force-response-1.0
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[012]" redirect-carefully
BrowserMatch "^gnome-vfs" redirect-carefully
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName 143.146.254.7
        SSLEngine on
        SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
        SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
        SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
    RewriteEngine on
        RewriteRule ^/(login_form)$ https://143.146.253.7/$1/$2 [R,noescape]
        RewriteRule http://143.146.254.7:8080/VirtualHostBase/https/143.146.253.7:443/VirtualHostRoot/$1 [P,L]
</VirtualHost>
</IfModule>

```

A.3 File contents of ssl.conf

The file `/etc/httpd/conf/ssl.conf` is a file that controls the SSL mechanism and it must be modified for the correct functioning of *Apache*'s SSL features. According to [\[7\]](#) [\[8\]](#) [\[9\]](#) [\[10\]](#) [\[11\]](#) [\[12\]](#), the following changes must be made to the file `/etc/httpd/conf/ssl.conf`:

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
SSLPassPhraseDialog builtin
SSLSessionCache shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout 300
SSLMutex default
SSLRandomSeed startup file:/dev/urandom 256
SSLRandomSeed connect builtin
SSLCryptoDevice builtin
<VirtualHost _default_:443>
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn
SSLEngine on
RewriteEngine on
RewriteRule ^(login_form)$ https://143.146.253.7/$1/$2 [R,noescape]
RewriteRule ^/(.*) http://
143.146.253.7:8080/VirtualHostBase/https/143.146.253.7:443/VirtualHostRoot/$1 [P,L]
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
```

```
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

Annex B Nessus security scan report

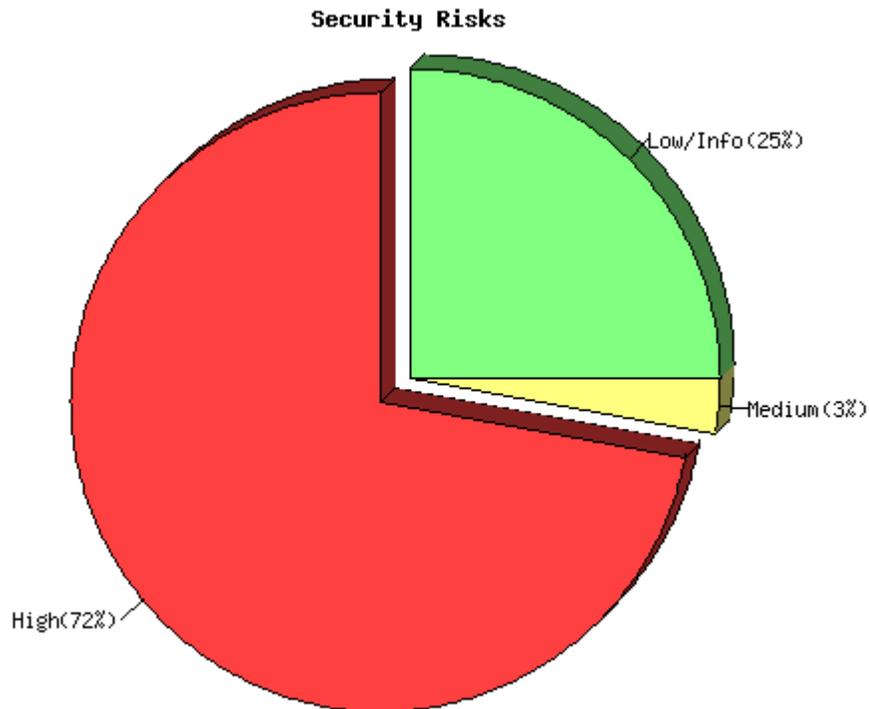
B.1 Part I of the Nessus report

Nessus Report

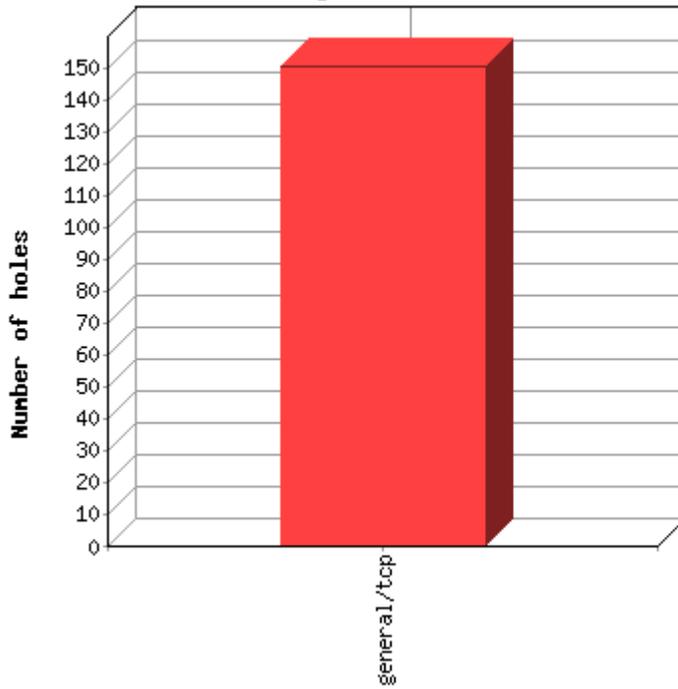
The Nessus Security Scanner was used to assess the security of 1 host

- **150 security holes have been found**
 - **6 security warnings have been found**
 - **52 security notes have been found**
-

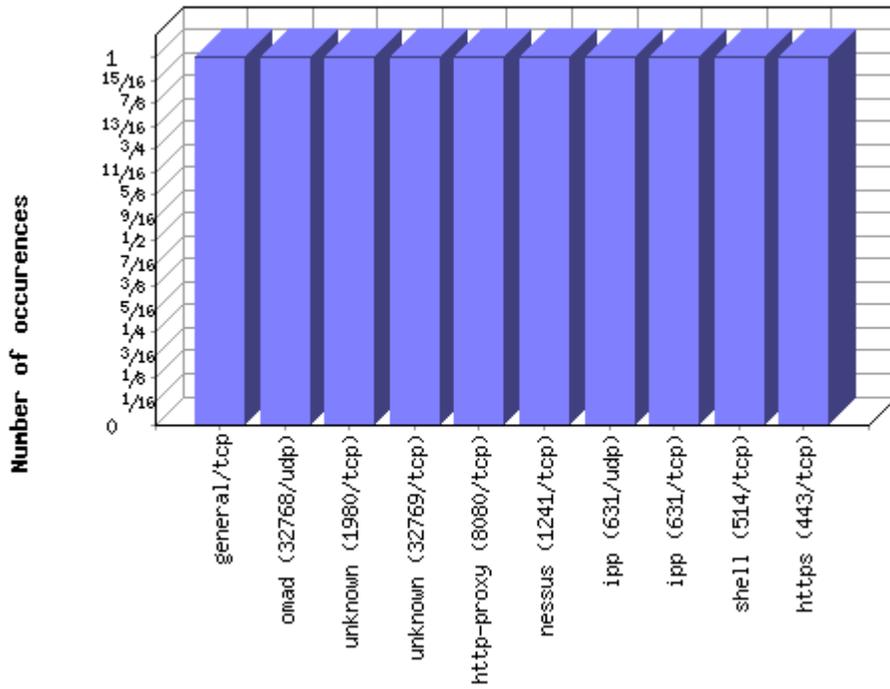
Part I: Graphical Summary :



Most dangerous services on the network :



Services that are the most present on the network :



Part II. Results, by host:

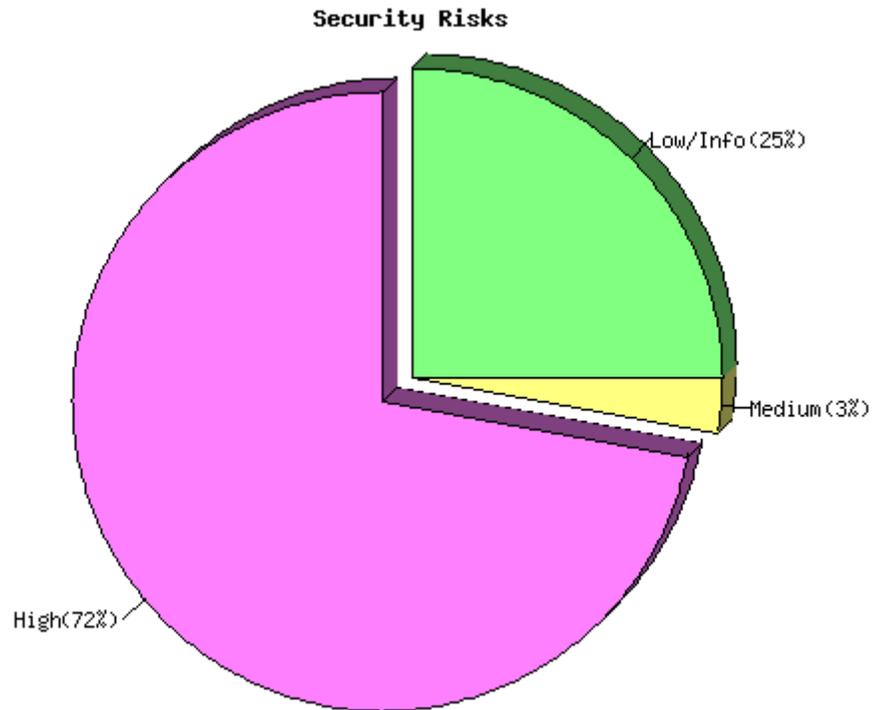
[localhost](#) (found 150 security holes)

This file was generated by [Nessus](#), the open-sourced security scanner.

B.2 Part II of the Nessus report

Nessus Scan: localhost

Repartition of the level of the security problems:



List of open ports:

- [ssh \(22/tcp\)](#) (Security warnings found)
- [telnet \(23/tcp\)](#) (Security warnings found)
- [http \(80/tcp\)](#) (Security warnings found)
- [sunrpc \(111/tcp\)](#) (Security notes found)

- [sunrpc \(111/udp\)](#) (Security notes found)
- [auth \(113/tcp\)](#) (Security warnings found)
- [https \(443/tcp\)](#) (Security warnings found)
- [shell \(514/tcp\)](#) (Security warnings found)
- [ipp \(631/tcp\)](#) (Security notes found)
- [ipp \(631/udp\)](#)
- [nessus \(1241/tcp\)](#) (Security notes found)
- [http-proxy \(8080/tcp\)](#) (Security notes found)
- [unknown \(32769/tcp\)](#) (Security notes found)
- [unknown \(1980/tcp\)](#) (Security notes found)
- [omad \(32768/udp\)](#) (Security notes found)
- [general/tcp](#) (Security hole found)

Warning found on port ssh (22/tcp)

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution :

If you use OpenSSH, set the option 'Protocol' to '2'

If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

Risk factor : Low

Nessus ID : [10882](#)

Information found on port ssh (22/tcp)

Nmap has identified this service as OpenSSH 3.9p1 (protocol 1.99)

Nessus ID : [14259](#)

Information found on port ssh (22/tcp)

An ssh server is running on this port

Nessus ID : [10330](#)

Information found on port ssh (22/tcp)

Remote SSH version : SSH-1.99-OpenSSH_3.9p1

Remote SSH supported authentication : publickey,gssapi-with-mic,password

Nessus ID : [10267](#)

Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.33
- . 1.5
- . 1.99
- . 2.0

SSHv1 host key fingerprint : 14:03:04:29:08:8c:fb:a7:54:f9:c8:46:80:f5:5d:e6

SSHv2 host key fingerprint : db:66:a9:2c:22:71:04:1a:2f:a1:d1:52:75:d0:c0:f5

Nessus ID : [10881](#)

Warning found on port telnet (23/tcp)

Synopsis :

A telnet server is listening on the remote port

Description :

The remote host is running a telnet server.
Using telnet is not recommended as logins, passwords and commands are transferred in clear text.

An attacker may eavesdrop on a telnet session and obtain the credentials of other users.

Solution :

Disable this service and use SSH instead

Risk factor :

Medium / CVSS Base Score : 4
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:C)

Plugin output:

Remote telnet banner:
Fedora Core release 3 (Heidelberg)
Kernel 2.6.9-1.667 on an i686
login:
Nessus ID : [10281](#)

Information found on port telnet (23/tcp)

Nmap has identified this service as Linux telnetd
Nessus ID : [14259](#)

Information found on port telnet (23/tcp)

identd reveals that this service is running as user
[U2FsdGVkX1/uXEpo6PmZpfMATQwtL9x2BqYp1aroBoo=]

Nessus ID : [14272](#)

Information found on port telnet (23/tcp)

A telnet server seems to be running on this port
Nessus ID : [10330](#)

Information found on port telnet (23/tcp)

The Telnet service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

Solution:

If you are running a Unix-type system, OpenSSH can be used instead of telnet. For Unix systems, you can comment out the 'telnet' line in /etc/inetd.conf. For Unix systems which use xinetd, you will need to modify the telnet services file in the /etc/xinetd.d folder. After making any changes to xinetd or inetd configuration files, you must restart the service in order for the changes to take affect.

In addition, many different router and switch manufacturers support SSH as a telnet replacement. You should contact your vendor for a solution which uses an encrypted session.

Risk factor : Low

CVE : [CVE-1999-0619](#)

Nessus ID : [10280](#)

Warning found on port http (80/tcp)

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, Nessus was able to determine that is is running :
Zope/(Zope 2.7.5-1.fc3, python 2.3.4, linux2) ZServer/1.1 Plone/2.0.5

Risk factor : None

Solution : Fix your configuration.

Nessus ID : [11239](#)

Information found on port http (80/tcp)

A web server is running on this port
Nessus ID : [10330](#)

Information found on port http (80/tcp)

Nessus was not able to reliably identify this server. It might be:
AppleShareIP/6.0.0
The fingerprint differs from these known signatures on 6 point(s)

Nessus ID : [11919](#)

Information found on port sunrpc (111/tcp)

The RPC service rpcbind is running on this port
If you do not use it, disable it, as it is
a potential security risk
Nessus ID : [14259](#)

Information found on port sunrpc (111/tcp)

Nmap has identified this service as rpc #100000 V2
Nessus ID : [14259](#)

Information found on port sunrpc (111/tcp)

identd reveals that this service is running as user
[U2FsGVkX19wDlfdjoexmeKCR1Ml0Oc4bHU47D2sxxM=]
Nessus ID : [14272](#)

Information found on port sunrpc (111/tcp)

The RPC portmapper is running on this port.

An attacker may use it to enumerate your list
of RPC services. We recommend you filter traffic
going to this port.

Risk factor : Low
CVE : [CVE-1999-0632](#), [CVE-1999-0189](#)
BID : [205](#)
Nessus ID : [10223](#)

Information found on port sunrpc (111/tcp)

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

Nessus ID : [11111](#)

Information found on port sunrpc (111/udp)

The RPC service rpcbind is running on this port
If you do not use it, disable it, as it is
a potential security risk
Nessus ID : [14259](#)

Information found on port sunrpc (111/udp)

Nmap has identified this service as rpc #100000 V2
Nessus ID : [14259](#)

Information found on port sunrpc (111/udp)

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

Nessus ID : [11111](#)

Warning found on port auth (113/tcp)

The service on this port should have been already identified
by other plugins.
find_service2 worked around this but your report might be incomplete.
You should increase the read timeout and rerun Nessus against this
target
Nessus ID : [11153](#)

Information found on port auth (113/tcp)

identd reveals that this service is running as user
[U2FsdGVkX1+jVtav0Naud0nReAtJovc/YU/UM/EeceY=]

Nessus ID : [14272](#)

Information found on port auth (113/tcp)

An unknown service is running on this port.
It is usually reserved for AUTH
Nessus ID : [10330](#)

Information found on port auth (113/tcp)

An Auth/ident server seems to be running on this port
Nessus ID : [11153](#)

Information found on port auth (113/tcp)

The remote ident server returns random token instead of leaking real user IDs. This is a good thing.

Risk factor: None
Nessus ID : [18373](#)

Information found on port auth (113/tcp)

The remote host is running an ident (also known as 'auth') daemon.

The 'ident' service provides sensitive information to potential attackers. It mainly says which accounts are running which services. This helps attackers to focus on valuable services (those owned by root). If you do not use this service, disable it.

Solution : Under Unix systems, comment out the 'auth' or 'ident' line in /etc/inetd.conf and restart inetd

Risk factor : Low
CVE : [CVE-1999-0629](#)
Nessus ID : [10021](#)

Warning found on port https (443/tcp)

It seems that your web server tries to hide its version or name, which is a good thing. However, using a special crafted request, Nessus was able to determine that is is running :
Apache/2.0.52 (Fedora)

Risk factor : None
Solution : Fix your configuration.
Nessus ID : [11239](#)

Information found on port https (443/tcp)

Nmap has identified this service as Apache httpd 2.0.52 ((Fedora))
Nessus ID : [14259](#)

Information found on port https (443/tcp)

A SSLv2 server answered on this port
Nessus ID : [10330](#)

Information found on port https (443/tcp)

A web server is running on this port through SSL
Nessus ID : [10330](#)

Information found on port https (443/tcp)

Nessus was not able to reliably identify this server. It might be:
Apache/1.3.14 (Unix) Resin/2.1.4 PHP/4.0.4pl1
The fingerprint differs from these known signatures on 8 point(s)
Nessus ID : [11919](#)

Information found on port https (443/tcp)

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,

OU=SomeOrganizationalUnit,

CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Validity

Not Before: Aug 25 12:48:05 2005 GMT

Not After : Aug 25 12:48:05 2006 GMT

Subject: C=--, ST=SomeState, L=SomeCity, O=SomeOrganization,

OU=SomeOrganizationalUnit,

CN=localhost.localdomain/emailAddress=root@localhost.localdomain

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:c9:6e:a0:e2:98:a4:5f:12:58:2a:bb:65:b3:bf:

f8:18:b6:fe:12:c2:04:93:d0:34:4d:dc:ed:b7:21:

e9:83:b1:f8:91:5a:c4:fa:e0:0f:0c:e3:aa:0c:a0:

b7:2b:71:2d:1e:7b:0b:55:73:07:0e:99:88:47:b6:

11:4f:42:88:da:d7:15:f1:06:be:71:01:4a:a8:0b:

82:ab:2a:d6:21:66:96:7c:50:9a:3c:33:bd:a8:25:

3f:64:da:4e:1b:ad:31:cf:04:d6:f7:25:c7:99:57:

5f:44:17:83:8f:85:ac:20:b6:c2:34:b8:47:54:b4:

ea:8e:c9:0f:33:a2:b4:06:33

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

B9:9A:13:0E:F2:BB:26:9D:D8:E5:A8:58:5D:A3:DF:D8:F1:3A:21:85

X509v3 Authority Key Identifier:

keyid:B9:9A:13:0E:F2:BB:26:9D:D8:E5:A8:58:5D:A3:DF:D8:F1:3A:21:85

DirName:/C=--

/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/CN=l

ocalhost.localdomain/emailAddress=root@localhost.localdomain

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

a5:88:8d:ba:f0:ac:7b:ef:ac:35:34:96:a1:15:f7:f3:47:8f:

51:b8:1a:70:99:04:c4:91:42:0a:8e:83:cd:e4:c2:33:3f:99:

9a:26:5e:3e:01:d9:8a:9f:53:7f:43:23:ad:33:94:45:24:54:
dc:58:8a:8e:20:c9:8a:7d:14:43:98:a9:98:12:f1:90:37:db:
15:a7:7f:20:6a:35:60:72:ab:ea:cd:36:a4:f0:61:c9:a6:f6:
8d:1b:fe:ad:70:f1:97:62:0f:9f:a5:98:ec:1a:dc:d7:24:89:
de:a8:58:fc:7e:f2:f9:31:dc:67:59:8c:fd:79:5a:34:9c:d9:
2a:a8

Here is the list of available SSLv2 ciphers:

RC4-MD5

EXP-RC4-MD5

RC2-CBC-MD5

EXP-RC2-CBC-MD5

DES-CBC-MD5

DES-CBC3-MD5

RC4-64-MD5

The SSLv2 server offers 5 strong ciphers, but also
0 medium strength and 2 weak "export class" ciphers.

The weak/medium ciphers may be chosen by an export-grade
or badly configured client software. They only offer a
limited protection against a brute force attack

Solution: disable those ciphers and upgrade your client
software if necessary.

See <http://support.microsoft.com/default.aspx?scid=kb;en-us;216482>

or http://httpd.apache.org/docs-2.0/mod/mod_ssl.html#sslciphersuite

This SSLv2 server also accepts SSLv3 connections.

This SSLv2 server also accepts TLSv1 connections.

Nessus ID : [10863](#)

Information found on port https (443/tcp)

Synopsis :

The remote service encrypts traffic using a protocol with known
weaknesses.

Description :

The remote service accepts connections encrypted using SSL 2.0, which
reportedly suffers from several cryptographic flaws and has been
deprecated for several years. An attacker may be able to exploit these
issues to conduct man-in-the-middle attacks or decrypt communications
between the affected service and clients.

See also :

<http://www.schneier.com/paper-ssl.pdf>

Solution :

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Nessus ID : [20007](#)

Warning found on port shell (514/tcp)

The rsh service is running.

This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. It is a built-in backdoor into a system that an attacker will make easy use of.

You should disable this service and use ssh instead.

Solution : Comment out the 'rsh' line in /etc/inetd.conf.

Risk factor : Low

CVE : [CVE-1999-0651](#)

Nessus ID : [10245](#)

Information found on port ipp (631/tcp)

Nmap has identified this service as CUPS 1.1

Nessus ID : [14259](#)

Information found on port ipp (631/tcp)

identd reveals that this service is running as user
[U2FsdGVkX18LvT3u2HvHvMPn6QilACXBghAP+mBcIxs=]

Nessus ID : [14272](#)

Information found on port ipp (631/tcp)

A web server is running on this port
Nessus ID : [10330](#)

Information found on port ipp (631/tcp)

Nessus was not able to reliably identify this server. It might be:
CUPS/1.1
The fingerprint differs from these known signatures on 7 point(s)

Nessus ID : [11919](#)

Information found on port ipp (631/tcp)

The remote web server type is :

CUPS/1.1

Nessus ID : [10107](#)

Information found on port nessus (1241/tcp)

identd reveals that this service is running as user
[U2FsdGVkX1+nU6+08QIvNKEgHFOFLQcJv/ygqVC5pnE=]

Nessus ID : [14272](#)

Information found on port nessus (1241/tcp)

A TLSv1 server answered on this port

Nessus ID : [10330](#)

Information found on port nessus (1241/tcp)

Synopsis :

A Nessus daemon is listening on the remote port.

Description :

A Nessus daemon is listening on the remote port. It is not recommended to let anyone connect to this port.

Also, make sure that the remote Nessus installation has been authorized.

Solution :

Filter incoming traffic to this port.

Risk factor :

None

Nessus ID : [10147](#)

Information found on port http-proxy (8080/tcp)

A web server is running on this port

Nessus ID : [10330](#)

Information found on port http-proxy (8080/tcp)

Nessus was not able to reliably identify this server. It might be:

Zope/(Zope 2.7.0, python 2.3.4, linux2) ZServer/1.1

Zope/(Zope 2.5.1-2.7.0)

SlimServer 5.1

Zope 2.5.to 2.7

The fingerprint differs from these known signatures on 7 point(s)

Nessus ID : [11919](#)

Information found on port http-proxy (8080/tcp)

The remote web server type is :

Medusa/1.35.8.2

Nessus ID : [10107](#)

Information found on port unknown (32769/tcp)

identd reveals that this service is running as user
[U2FsdGVkX19+WYPixt1T+9Rj1EAl+e4oGkaQROh3IP8=]

Nessus ID : [14272](#)

Information found on port unknown (32769/tcp)

RPC program #100024 version 1 'status' is running on this port

Nessus ID : [11111](#)

Information found on port unknown (1980/tcp)

identd reveals that this service is running as user
[U2FsdGVkX1+R3f185NcjxY9B3kY5z5MtBeYVEdV6fcc=]

Nessus ID : [14272](#)

Information found on port unknown (1980/tcp)

A web server is running on this port

Nessus ID : [10330](#)

Information found on port unknown (1980/tcp)

Nessus was not able to reliably identify this server. It might be:
SlimServer 5.1
webfs/1.20
The fingerprint differs from these known signatures on 9 point(s)

Nessus ID : [11919](#)

Information found on port unknown (1980/tcp)

The remote web server type is :

Medusa/1.35.8.2

Nessus ID : [10107](#)

Information found on port omad (32768/udp)

RPC program #100024 version 1 'status' is running on this port

Nessus ID : [11111](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-993 (lynx).

Lynx is a text-based Web browser. Lynx does not display any images, but it does support frames, tables, and most other HTML tags. One advantage Lynx has over graphical browsers is speed; Lynx starts and exits quickly and swiftly displays webpages.

Update Information:

This package fixes a security bug (CVE-2005-3120) when handling connections to NNTP (news) servers.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-3120](#)
Nessus ID : [20027](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-369 (gaim).

Gaim allows you to talk to anyone using a variety of messaging protocols, including AIM (Oscar and TOC), ICQ, IRC, Yahoo!, MSN Messenger, Jabber, Gadu-Gadu, Napster, and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor.

Gaim supports many common features of other clients, as well as many unique features, such as perl scripting and C plugins.

Gaim is NOT affiliated with or endorsed by America Online, Inc., Microsoft Corporation, or Yahoo! Inc. or other messaging service providers.

Update Information:

Many bug fixes and two important security fixes.

Solution : <http://www.fedoranews.org/blog/index.php?p=662>
Risk factor : High
CVE : [CVE-2005-1261](#), [CVE-2005-1262](#)
Nessus ID : [18336](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-254 (epiphany).

epiphany is a simple GNOME web browser based on the Mozilla rendering engine

Update Information:

There were several security flaws found in the mozilla package, which epiphany depends on. Users of epiphany are advised to upgrade to this

updated package which has been rebuilt against a later version of mozilla which is not vulnerable to these flaws.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19636](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-727 (netpbm).

The netpbm package contains a library of functions that support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps), and others.

Update Information:

pstopnm in netpbm does not properly use the '-dSAFER' option when calling Ghostscript to convert a PostScript file into a (1) PBM, (2) PGM, or (3) PNM file, which allows external user-complicit attackers to execute arbitrary commands.

Solution : <http://www.fedoranews.org/blog/index.php?p=847>
Risk factor : High
CVE : [CVE-2005-2471](#)
Nessus ID : [19465](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-124 (postgresql).

PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions).

* Mon Feb 07 2005 Tom Lane 7.4.7-1.FC3.2

- Put regression tests under /usr/lib64 on 64-bit archs, since .so files

are not architecture-independent.

* Mon Feb 07 2005 Tom Lane 7.4.7-1.FC3.1

- Update to PostgreSQL 7.4.7 (fixes CVE-2005-0227 and other issues).
- Update to PyGreSQL 3.6.1.
- Add versionless symlinks to jar files (bz#145744)
- Add restorecon to postgresql.init in order to restore database to correct SELinux context.

Solution : <http://www.fedoranews.org/blog/index.php?p=374>

Risk factor : High

CVE : [CVE-2005-0227](#)

Nessus ID : [16353](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-136 (xpdf).

Xpdf is an X Window System based viewer for Portable Document Format (PDF) files. Xpdf is a small and efficient program which uses standard X fonts.

* Wed Feb 09 2005 Than Ngo

1:3.00-10.4

- More fixing of CVE-2004-0888 patch (bug #135393, #147524)

Solution : <http://www.fedoranews.org/blog/index.php?p=382>

Risk factor : High

CVE : [CVE-2004-0888](#)

Nessus ID : [16358](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-082 (openswan).

Openswan is a free implementation of IPSEC & IKE for Linux.

IPsec is Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN.

This package contains the daemons and userland tools for setting up Openswan on a kernel with the 2.6 native IPsec code.

Update Information:

This erratum fixes the remote exploitation of a stack based buffer overflow vulnerability in Xelerance Corp.'s Openswan, which could allow attackers to execute arbitrary code.

The vulnerability specifically exists due to a lack of bounds checking in the pluto application when Openswan is compiled with XAUTH and PAM support.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-0162 to this problem.

Solution : <http://www.fedoranews.org/blog/index.php?p=336>

Risk factor : High

CVE : [CVE-2005-0162](#)

Nessus ID : [16285](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-990 (texinfo).

Texinfo is a documentation system that can produce both online information and printed output from a single source file. The GNU Project uses the Texinfo file format for most of its documentation.

Install texinfo if you want a documentation system for producing both online and print documentation from the same source file and/or if you are going to write documentation for the GNU Project.

Update Information:

This package fixes a temporary file name vulnerability in the texindex program (CVE-2005-3011).

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-3011](#)
Nessus ID : [20025](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-025 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

CVE-2005-0001

Paul Starzetz from isec.pl found an exploitable hole in the x86 SMP page fault handler which could lead to privilege escalation.
<http://www.isec.pl/vulnerabilities/isec-0022-pagefault.txt>

This update additionally fixes a random memory corruption issue present in the previous update, and in addition updates to the latest -ac collection of patches. A full changelog of the update vs the previous -ac8 based release is available at <http://lkml.org/lkml/2005/1/13/219>

- * Thu Jan 13 2005 Dave Jones
 - Update to 2.6.10-ac9
 - Fix slab corruption in ACPI video code.
- * Mon Jan 10 2005 Dave Jones
 - Add another Lexar card reader to the whitelist. (#143600)
 - Package asm-m68k for asm-ppc includes. (don't ask). (#144604)

Solution : <http://www.fedoranews.org/blog/index.php?p=278>
Risk factor : High
CVE : [CVE-2005-0001](#)
Nessus ID : [16166](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-154 (squid).

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.

Update Information:

This update fixes
CVE-2005-0446 Squid DoS from bad DNS response

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0446](#)

Nessus ID : [19615](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-472 (sudo).

Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.

* Tue Jun 21 2005 Karel Zak 1.6.7p5-30.3

- fix #161116 - CVE-2005-1993 sudo trusted user arbitrary command execution

Solution : <http://www.fedoranews.org/blog/index.php?p=727>
Risk factor : High
CVE : [CVE-2005-1993](#)
Nessus ID : [18542](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-690 (ethereal).

Ethereal is a network traffic analyzer for Unix-ish operating systems.

This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, and contains plugins and documentation for ethereal. A graphical user interface is packaged separately to GTK+ package.

Update Information:

To reduce the risk of future vulnerabilities in Ethereal, the ethereal and tethereal programs in this update have been compiled as Position Independent Executables (PIE).

Solution : <http://www.fedoranews.org/blog/index.php?p=804>
Risk factor : High
Nessus ID : [19379](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-329 (HelixPlayer).

The Helix Player 1.0 is an open-source media player built in the Helix Community for consumers. Built using GTK, it plays open source formats, like Ogg Vorbis and Theora using the powerful Helix DNA Client Media Engine.

Update Information:

Solution : Get the newest Fedora Updates

Risk factor : High
Nessus ID : [19653](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-148 (kdeedu).

Educational/Edutainment applications for KDE

* Tue Feb 8 2005 Than Ngo
3.3.1-2.3

- More fixing of CVE-2005-0011 patch

* Tue Feb 1 2005 Than Ngo
3.3.1-2.2

- Apply patch to fix buffer overflow in fliccd, CVE-2005-0011
(#146290)
- replace kgeo (#142367)

Solution : <http://www.fedoranews.org/blog/index.php?p=403>
Risk factor : High
CVE : [CVE-2005-0011](#)
Nessus ID : [17137](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-955 (abiword).

AbiWord is a cross-platform Open Source word processor. The goal is to make AbiWord full-featured, and remain lean.

Update Information:

Chris Evans discovered a buffer overflow in AbiWord's RTF importer

Solution : Get the newest Fedora Updates
Risk factor : High

CVE : [CVE-2005-2964](#)
Nessus ID : [19882](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-848 (httpd).

Apache is a powerful, full-featured, efficient, and freely-available Web server. Apache is also the most popular Web server on the Internet.

Update Information:

This update includes two security fixes. An issue was discovered in mod_ssl where 'SSLVerifyClient require' would not be honoured in location context if the virtual host had 'SSLVerifyClient optional' configured (CVE-2005-2700). An issue was discovered in memory consumption of the byterange filter for dynamic resources such as PHP or CGI script (CVE-2005-2728).

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2700](#), [CVE-2005-2728](#)
Nessus ID : [19727](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-276 (squid).

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.

Note that squid-2.5.STABLE7 and later do not use /etc/squid/errors for error messages. If you do not want to use the default English error

messages, you must set the `error_directory` in your `/etc/squid/squid.conf` to the appropriate subdirectory of `/usr/share/squid/errors`

* Wed Mar 23 2005 Jay Fenlason <fenlason redhat com> 7:2.5.STABLE9-1.FC3.4

- Add more upstream patches.
- add the `-libbind` patch, to avoid picking up a new dependency on `libbind`.
- Remove references to `/etc/squid/errors` from this spec, since squid now uses `{_datadir}/squid/errors/English/` by default (overridable in `/etc/squid/squid.conf`, as always)
- mark `{_datadir}/squid/errors` as `config(noreplace)` so custom error messages won't get stomped on.

* Wed Mar 16 2005 Jay Fenlason <fenlason redhat com> 7:2.5.STABLE9-1.FC3.3

- Actually apply the `-date` patch.

* Wed Mar 16 2005 Jay Fenlason <fenlason redhat com> 7:2.5.STABLE9-1.FC3.2

- New upstream version, with 14 patches. Includes fix for `bz#150234` cookie leak in squid

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19643](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-353 (perl).

Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts.

Install this package if you want to program in Perl or enable your system to handle Perl scripts.

Update Information:

Security and packaging fixes.

Solution : <http://www.fedoranews.org/blog/index.php?p=638>

Risk factor : High

CVE : [CVE-2004-0452](#), [CVE-2005-0156](#)

Nessus ID : [18335](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-497 (binutils).

Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

* Wed Jun 29 2005 Jakub Jelinek 2.15.92.0.2-5.1

- bfd and readelf robustification (CVE-2005-1704, #158680)

- fix buffer overflows in readelf (#149506)

Solution : <http://www.fedoranews.org/blog/index.php?p=735>

Risk factor : High

CVE : [CVE-2005-1704](#)

Nessus ID : [18593](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-351 (tcpdump).

Tcpdump is a command-line tool for monitoring network traffic.

Tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria.

Install tcpdump if you need a program to monitor network traffic.

* Fri Apr 29 2005 Martin Stransky <stransky redhat com> - 14:3.8.2-8.FC3

- fix for CVE-2005-1280 Multiple DoS issues in tcpdump (CVE-2005-1279 CVE-2005-1278), #156040

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-1278](#), [CVE-2005-1280](#)

Nessus ID : [19657](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-550 (kdelibs).

Libraries for the K Desktop Environment:

KDE Libraries included: kdcORE (KDE core library), kdeui (user interface),

kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking),

kspell (spelling checker), jscript (javascript), kab (addressbook),

kingio (image manipulation).

* Tue Dec 14 2004 Than Ngo

3.3.1-2.4.FC3

- apply the patch to fix Konqueror Window Injection Vulnerability #142510

CVE-2004-1158, Thanks to KDE security team

* Fri Dec 10 2004 Than Ngo

3.3.1-2.3.FC3

- Security Advisory: plain text password exposure, #142487
thanks to KDE security team

Solution : <http://www.fedoranews.org/blog/index.php?p=200>
Risk factor : High
CVE : [CVE-2004-1158](#)
Nessus ID : [15979](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-403 (ruby).

Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.

* Thu Nov 11 2004 Akira TAGOH - 1.8.1-7.FC3.1

- security fix [CVE-2004-0983]
- security fix [CVE-2004-0755]
- ruby-1.8.1-cgi-dos.patch: applied to fix a denial of service issue. (#138366)
- ruby-1.8.1-cgi_session_perms.patch: sets the permission of the session data file to 0600. (#130063)

* Sat Oct 30 2004 Akira TAGOH - 1.8.1-7.fc3

- added openssl-devel and db4-devel into BuildRequires. (#137479)

Solution : <http://www.fedoranews.org/blog/index.php?p=63>
Risk factor : High
CVE : [CVE-2004-0755](#), [CVE-2004-0983](#)
Nessus ID : [15731](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-625 (zlib).

Zlib is a general-purpose, patent-free, lossless data compression library which is used by many different programs.

* Fri Jul 22 2005 Ivana Varekova 1.2.1.2-3.fc3
- fix bug 163038 - CVE-2005-1849 - zlib overflow problem

Solution : <http://www.fedoranews.org/blog/index.php?p=784>
Risk factor : High
CVE : [CVE-2005-1849](#)
Nessus ID : [19293](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-273 (xorg-x11).

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality which full fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed upon.

Update Information:

An integer overflow flaw was found in libXpm, which is used by some applications for loading of XPM images. An attacker could create a malicious XPM file that would execute arbitrary code if opened by a victim using an application linked to the vulnerable library. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0605 to this issue.

Futhermore, this updates the Fedora Core 3 X.org packages to the 6.8.2 maintenance release, which includes a large number of bug fixes:

[14]<http://xorg.freedesktop.org/wiki/X11R682Release>

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0605](#)
Nessus ID : [19641](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-404 (mikmod).

MikMod is one of the best and most well known MOD music file players for UNIX-like systems. This particular distribution is intended to compile fairly painlessly in a Linux environment. MikMod uses the OSS /dev/dsp driver including all recent kernels for output, and will also write .wav files. Supported file formats include MOD, STM, S3M, MTM, XM, ULT, and IT. The player uses ncurses for console output and supports transparent loading from gzip/pkzip/zoo archives and the loading/saving of playlists.

Install the mikmod package if you need a MOD music file player.

* Mon Jun 06 2005 Martin Stransky 3.1.6-31.FC3

- fixed #159290,#159291 - CVE-2003-0427
- fixed playing mod files from tar archive

Solution : <http://www.fedoranews.org/blog/index.php?p=715>

Risk factor : High

CVE : [CVE-2003-0427](#)

Nessus ID : [18438](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-249 (mozilla).

Mozilla is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

Multiple bugs have been found in Mozilla.

Users of Mozilla are advised to upgrade to this updated package which contains Mozilla version 1.7.6 to correct these issues.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0233](#), [CVE-2005-0399](#), [CVE-2005-0401](#), [CVE-2005-0585](#)

Nessus ID : [19634](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-841 (perl-DBI).

DBI is a database access Application Programming Interface (API) for the Perl programming language. The DBI API specification defines a set of functions, variables and conventions that provide a consistent database interface independent of the actual database being used.

Update Information:

Old and low priority security update that we forgot to push a while ago.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19725](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-809 (php).

PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The mod_php module enables the Apache Web server to understand and process the embedded PHP language in Web pages.

Update Information:

This update includes the latest upstream version of the PEAR XML_RPC package, which fixes a security issue in request parsing in the XML_RPC Server code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2498 to this issue.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2498](#)
Nessus ID : [19667](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-106 (squid).

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.

* Tue Feb 01 2005 Jay Fenlason 7:2.5.STABLE7-1.FC3.1

- Add more upstream patches, including fixes for bz#146783 Correct handling of oversized reply headers
bz#146778 CVE-2005-0211 Buffer overflow in WCCP recvfrom() call

* Thu Jan 20 2005 Jay Fenlason 7:2.5.STABLE7-1.FC3

- Upgrade to 2.5.STABLE7 and 18 upstream patches.
- This includes fixes for CVE-2005-0094 CVE-2005-0095 CVE-2004-0096 and CVE-2004-0097. This closes bz#145543 and bz#141938
- This obsoletes Ulrich Drepper's -nonbl patch.
- Add a triggerin on samba-common to make /var/cache/samba/winbindd_privileged accessible so that ntlm_auth will work.
This fixes bz#103726

Solution : <http://www.fedoranews.org/blog/index.php?p=357>

Risk factor : High

CVE : [CVE-2004-0096](#), [CVE-2004-0097](#), [CVE-2005-0211](#)

Nessus ID : [16289](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-392 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of

any

Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

- * Tue May 17 2005 Dave Jones
 - Remove the unused (and outdated) Xen patches from the FC3 tree.
- * Mon May 16 2005 Dave Jones
 - Rebase to 2.6.11.10, (fixing CVE-2005-1264)
- * Thu May 12 2005 Dave Jones
 - Rebase to 2.6.11.9, (fixing CVE-2005-1263)
- * Tue May 10 2005 Dave Jones
 - Fix two bugs in x86-64 page fault handler.
- * Mon May 9 2005 Dave Jones
 - Rebase to 2.6.11.8
 - | Fixes CVE-2005-1368 (local DoS in key lookup). (#156680)
 - | Fixes CVE-2005-1369 (i2c alarms sysfs DoS). (#156683)
 - Merge IDE fixes from 2.6.11-ac7
 - Add Conflicts for older IPW firmwares.
 - Fix conntrack leak with raw sockets.
- * Sun May 1 2005 Dave Jones
 - Various firewire fixes backported from -mm. (#133798)
 - (Thanks to Jody McIntyre for doing this)
- * Fri Apr 29 2005 Dave Jones
 - fix oops in aacraid open when using adaptec tools. (#148761)
 - Blacklist another brainless SCSI scanner. (#155457)
- * Thu Apr 21 2005 Dave Jones
 - Fix up SCSI queue locking. (#155472)
- * Tue Apr 19 2005 Dave Jones
 - SCSI tape security: require CAP_ADMIN for SG_IO etc. (#155355)
- * Mon Apr 18 2005 Dave Jones
 - Retry more aggressively during USB device initialization
- * Thu Apr 14 2005 Dave Jones
 - Build DRM modular. (#154769)
- * Fri Apr 8 2005 Dave Jones
 - Disable Longhaul driver (again).

Solution : <http://www.fedoranews.org/blog/index.php?p=695>

Risk factor : High

CVE : [CVE-2005-1263](#), [CVE-2005-1264](#), [CVE-2005-1368](#), [CVE-2005-1369](#)

Nessus ID : [18377](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-410 (gaim).

Gaim allows you to talk to anyone using a variety of messaging protocols, including AIM (Oscar and TOC), ICQ, IRC, Yahoo!, MSN Messenger, Jabber, Gadu-Gadu, Napster, and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor.

Gaim supports many common features of other clients, as well as many unique features, such as perl scripting and C plugins.

Gaim is NOT affiliated with or endorsed by America Online, Inc., Microsoft Corporation, or Yahoo! Inc. or other messaging service providers.

Update Information:

More bug and denial of service fixes.

Solution : <http://www.fedoranews.org/blog/index.php?p=723>

Risk factor : High

CVE : [CVE-2005-1934](#)

Nessus ID : [18508](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-638 (httpd).

Apache is a powerful, full-featured, efficient, and freely-available Web server. Apache is also the most popular Web server on the Internet.

Update Information:

This update includes version 2.0.53 of the Apache HTTP server, and also adds security fixes for CVE CVE-2005-2088 and CVE CVE-2005-1268.

Solution : <http://www.fedoranews.org/blog/index.php?p=802>
Risk factor : High
CVE : [CVE-2005-1268](#), [CVE-2005-2088](#)
Nessus ID : [19374](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-172 (gaim).

Gaim allows you to talk to anyone using a variety of messaging protocols, including AIM (Oscar and TOC), ICQ, IRC, Yahoo!, MSN Messenger, Jabber, Gadu-Gadu, Napster, and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor.

Gaim supports many common features of other clients, as well as many unique features, such as perl scripting and C plugins.

Gaim is NOT affiliated with or endorsed by America Online, Inc., Microsoft Corporation, or Yahoo! Inc. or other messaging service providers.

Update Information:

This update resolves another DoS issue in parsing malformed HTML, and a MSN related crash that folks were hitting often.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0208](#)
Nessus ID : [19621](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-140 (mod_python).

Mod_python is a module that embeds the Python language interpreter

within
the server, allowing Apache handlers to be written in Python.

Mod_python brings together the versatility of Python and the power of the Apache Web server for a considerable boost in flexibility and performance over the traditional CGI approach.

Update Information:

Graham Dumpleton discovered a flaw affecting the publisher handler of mod_python, used to make objects inside modules callable via URL. A remote user could visit a carefully crafted URL that would gain access to objects that should not be visible, leading to an information leak. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0088 to this issue.

This update includes a patch which fixes this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=392>

Risk factor : High

CVE : [CVE-2005-0088](#)

Nessus ID : [16374](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-771 (slocate).

Slocate is a security-enhanced version of locate. Just like locate, slocate searches through a central database (which is updated nightly) for files that match a given pattern. Slocate allows you to quickly find files anywhere on your system.

Update Information:

A carefully prepared directory structure could stop the updatedb file system scan, resulting in an incomplete slocate database. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2499 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=849>

Risk factor : High
CVE : [CVE-2005-2499](#)
Nessus ID : [19481](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-242 (mailman).

Mailman is software to help manage email discussion lists, much like Majordomo and Smartmail. Unlike most similar products, Mailman gives each mailing list a webpage, and allows users to subscribe, unsubscribe, etc. over the Web. Even the list manager can administer his or her list entirely from the Web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail <-> news gateways, and so on.

Documentation can be found in: `/usr/share/doc/mailman-2.1.5`

When the package has finished installing, you will need to perform some additional installation steps, these are described in:
`/usr/share/doc/mailman-2.1.5/INSTALL.REDHAT`

Update Information:

A cross-site scripting (XSS) flaw in the driver script of mailman prior to version 2.1.5 could allow remote attackers to execute scripts as other web users. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-1177 to this issue.

Users of mailman should update to this erratum package, which corrects this issue by turning on STEALTH_MODE by default and using `Utils.websafe()` to quote the html.

In addition this version of the rpm includes a utility script in `/usr/share/doc/mailman-*/contrib/migrate-fhs` that can be run if the user has installed an FC3 or FC4 mailman rpm over an older non-FHS compliant mailman installation. The script will aid in moving the file locations from the old directory structure to the new FHS mailman directory structure that are present in FC3, FC4, and RHEL4. Users who have installed mailman originally from FC3, FC4 or RHEL4 will not need to migration any file locations.

Solution : Get the newest Fedora Updates
Risk factor : High

CVE : [CVE-2004-1177](#), [CVE-2005-0202](#)
Nessus ID : [19630](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-741 (vim).

VIM (VIvisual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.

Update Information:

CVE-2005-2368

This update is supposed to fix GTK2 dependency problems of the vim-6.3.086-0.fc3 package.

Solution : <http://www.fedoranews.org/blog/index.php?p=818>

Risk factor : High

CVE : [CVE-2005-2368](#)

Nessus ID : [19436](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-330 (cvs).

CVS (Concurrent Version System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred.

CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.

* Mon Apr 18 2005 Martin Stransky <stransky redhat com> 1.11.17-6.FC3

- add security fix CVE-2005-0753 (Derek Price)

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0753](#)

Nessus ID : [19654](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-804 (epiphany).

epiphany is a simple GNOME web browser based on the Mozilla rendering engine

* Thu Aug 18 2005 Marco Pesenti Gritti <mpg@redhat.com> 1.4.9-0

- Update to 1.4.9

- Remove download patch (integrated upstream)

- Add the manual to the package

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19665](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-858 (openssh).

OpenSSH is OpenBSD's SSH (Secure SHell) protocol implementation. SSH replaces rlogin and rsh, to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. Public key authentication may be used for 'passwordless' access to servers.

This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.

Update Information:

This security update fixes CVE-2005-2798 and resolves a problem with X forwarding binding only on IPv6 address on certain circumstances.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2798](#)
Nessus ID : [19731](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-013 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

This update rebases the kernel to match the upstream 2.6.10 release, and adds a number of security fixes by means of adding the latest -ac patch.

Solution : <http://www.fedoranews.org/blog/index.php?p=263>
Risk factor : High
CVE : [CVE-2004-1235](#)
Nessus ID : [16133](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-203 (grip).

Grip is a GTK+ based front-end for CD rippers (such as cdparanoia and cdda2wav) and Ogg Vorbis encoders. Grip allows you to rip entire tracks or just a section of a track. Grip supports the CDDB protocol for accessing track information on disc database servers.

Update Information:

This fixes a buffer overflow when the CDDB server returns more than 16 matches.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19625](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-266 (gdk-pixbuf).

The gdk-pixbuf package contains an image loading library used with the GNOME GUI desktop environment. The GdkPixBuf library provides image loading facilities, the rendering of a GdkPixBuf into various formats (drawables or GdkRGB buffers), and a cache interface.

Update Information:

David Costanzo found a bug in the way gdk-pixbuf processes BMP images. It is possible that a specially crafted BMP image could cause a denial of service attack in applications linked against gdk-pixbuf. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0891 to this issue.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0891](#)
Nessus ID : [19639](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-617 (epiphany).

epiphany is a simple GNOME web browser based on the Mozilla rendering engine

Update Information:

Epiphany is a simple GNOME web browser based on the Mozilla rendering engine.

There were several security flaws found in the mozilla package, which epiphany depends on.

Users of epiphany are advised to upgrade to this updated package which has been rebuilt

against a version of mozilla not vulnerable to these flaws.

Solution : <http://www.fedoranews.org/blog/index.php?p=782>

Risk factor : High

Nessus ID : [19274](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-299 (gaim).

Gaim allows you to talk to anyone using a variety of messaging protocols, including AIM (Oscar and TOC), ICQ, IRC, Yahoo!, MSN Messenger, Jabber, Gadu-Gadu, Napster, and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor.

Gaim supports many common features of other clients, as well as many unique features, such as perl scripting and C plugins.

Gaim is NOT affiliated with or endorsed by America Online, Inc., Microsoft Corporation, or Yahoo! Inc. or other messaging service providers.

Update Information:

[14]<http://gaim.sourceforge.net/security/>

[15]<http://gaim.sourceforge.net/ChangeLog>

gaim-1.2.1 resolves CVE-2005-0965 and CVE-2005-0966 as well as some crashes in the jabber and yahoo protocols. Read upstream's pages above for more details.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0966](#)

Nessus ID : [19645](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-618 (devhelp).

A API document browser for GNOME 2.

Update Information:

Devhhelp is an API document browser for the GNOME environment.

There were several security flaws found in the mozilla package, which devhhelp depends on.

Users of devhhelp are advised to upgrade to this updated package which has been rebuilt against a version of mozilla not vulnerable to these flaws.

Solution : <http://www.fedoranews.org/blog/index.php?p=783>

Risk factor : High

Nessus ID : [19275](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-573 (xpdf).

Xpdf is an X Window System based viewer for Portable Document Format (PDF) files. Xpdf is a small and efficient program which uses standard X fonts.

Update Information:

This package fixes a buffer overflow which allows attackers to cause the xpdf application to crash, and possibly to execute arbitrary code. The Common Vulnerabilities and Exposures projects (cve.mitre.org) has assigned the name CVE-2004-1125 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=229>

Risk factor : High

CVE : [CVE-2004-1125](#)

Nessus ID : [16051](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-651 (ethereal).

Ethereal is a network traffic analyzer for Unix-ish operating systems.

This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, and contains plugins and documentation for ethereal. A graphical user interface is packaged separately to GTK+ package.

* Thu Jul 28 2005 Jindrich Novy 0.10.12-1.FC3.1
- update to 0.10.12
- package /usr/sbin/randpkt
- sync with cleanup patch (most of it applied upstream)
- the new release fixes CVE-2005-2361 up to CVE-2005-2367

Solution : <http://www.fedoranews.org/blog/index.php?p=796>
Risk factor : High
CVE : [CVE-2005-2367](http://www.fedoranews.org/blog/index.php?p=796)
Nessus ID : [19320](http://www.fedoranews.org/blog/index.php?p=796)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-001 (exim).

Exim is a mail transport agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. In style it is similar to Smail 3, but its facilities are more extensive, and in particular it has options for verifying incoming sender and recipient addresses, for refusing mail from specified hosts, networks, or senders, and for controlling mail relaying. Exim is in production use at quite a few sites, some of which move hundreds of thousands of messages per day.

Exiscan is compiled in to allow inbuilt scanning capability. See <http://duncanthrax.net/exiscan-acl/>

Update Information:

This erratum fixes two relatively minor security issues which were discovered in Exim in the last few weeks. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CVE-2005-0021 and CVE-2005-0022 to these, respectively.

1. The function `host_aton()` can overflow a buffer if it is presented with an illegal IPv6 address that has more than 8 components.
2. The second report described a buffer overflow in the function `spa_base64_to_bits()`, which is part of the code for SPA authentication. This code originated in the Samba project. The overflow can be exploited only if you are using SPA authentication.

Solution : <http://www.fedoranews.org/blog/index.php?p=252>
Risk factor : High
CVE : [CVE-2005-0021](#), [CVE-2005-0022](#)
Nessus ID : [16113](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-844 (unzip).

The unzip utility is used to list, test, or extract files from a zip archive. Zip archives are commonly found on MS-DOS systems. The zip utility, included in the zip package, creates zip archives. Zip and unzip are both compatible with archives created by PKWARE(R)'s PKZIP for MS-DOS, but the programs' options and default behaviors do differ in some respects.

Update Information:

This update fixes TOCTOU issue in unzip.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19726](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-791 (cvs).

CVS (Concurrent Version System) is a version control system that can

record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred.

CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.

* Tue Aug 23 2005 Martin Stransky <stransky redhat com> 1.11.17-7.FC3
- fix for #166366 - CVS temporary file issue

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19662](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-211 (sylpheed).

This program is an X based fast email client which has features like:

- o user-friendly and intuitive interface
- o integrated NetNews client (partially implemented)
- o ability of keyboard-only operation
- o Mew/Wanderlust-like key bind
- o multipart MIME
- o unlimited multiple account handling
- o message queueing
- o assortment function
- o XML-based address book

See /usr/share/doc/sylpheed*/README for more information.

* Tue Mar 15 2005 Akira TAGOH <tagoh redhat com> - 1.0.3-0.FC3

- New upstream release.

- contains the possible buffer overflow issue. (#150688)
CVE-2005-0667

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0667](#)
Nessus ID : [19626](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-246 (firefox).

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

A buffer overflow bug was found in the way Firefox processes GIF images. It is possible for an attacker to create a specially crafted GIF image, which when viewed by a victim will execute arbitrary code as the victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0399 to this issue. A bug was found in the way Firefox processes XUL content. If a malicious web page can trick a user into dragging an object, it is possible to load malicious XUL content. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0401 to this issue. A bug was found in the way Firefox bookmarks content to the sidebar. If a user can be tricked into bookmarking a malicious web page into the sidebar panel, that page could execute arbitrary programs. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0402 to this issue. Users of Firefox are advised to upgrade to this updated package which contains Firefox version 1.0.2 and is not vulnerable to these issues.

Additionally, there was a bug found in the way Firefox rendered some fonts, notably the Tahoma font while italicized. This issue has been filed as Bug 150041 (bugzilla.redhat.com). This updated package contains a fix for this issue.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0399](#), [CVE-2005-0401](#), [CVE-2005-0402](#)
Nessus ID : [19632](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-802 (pcre).

Perl-compatible regular expression library. PCRE has its own native API, but a set of 'wrapper' functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE; the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.

Update Information:

the new package includes a fix for a heap buffer overflow.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2491](#)
Nessus ID : [19663](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-908 (cups).

The Common UNIX Printing System provides a portable printing layer for UNIX operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.

Update Information:

A bug was found in the way CUPS processes malformed HTTP requests. It is possible for a remote user capable of connecting to the CUPS daemon to issue a malformed HTTP GET request which will cause CUPS to enter an infinite loop. This is CVE-2005-2874.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2874](#)
Nessus ID : [19870](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-412 (gd).

The gd graphics library allows your code to quickly draw images complete with lines, arcs, text, multiple colors, cut and paste from other images, and flood fills, and to write out the result as a PNG or JPEG file. This is particularly useful in Web applications, where PNG and JPEG are two of the formats accepted for inline images by most browsers. Note that gd is not a paint program.

Update Information:

Several buffer overflows were reported in various memory allocation calls.

An attacker could create a carefully crafted image file in such a way that it could cause ImageMagick to execute arbitrary code when processing the image. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-0990 to these issues.

Whilst researching the fixes to these overflows, additional buffer overflows were discovered in calls to gdMalloc. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-0941 to these issues.

Users of gd should upgrade to these updated packages, which contain a backported security patch, and are not vulnerable to these issues.

Solution : <http://www.fedoranews.org/blog/index.php?p=69>
Risk factor : High
CVE : [CVE-2004-0941](#), [CVE-2004-0990](#)
Nessus ID : [15733](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-931 (firefox).

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

An updated firefox package that fixes several security bugs is now available for Fedora Core 3.

This update has been rated as having critical security impact by the Fedora Security Response Team.

Mozilla Firefox is an open source Web browser.

A bug was found in the way Firefox processes XBM image files. If a user views a specially crafted XBM file, it becomes possible to execute arbitrary code as the user running Firefox. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2701 to this issue.

A bug was found in the way Firefox processes certain Unicode sequences. It may be possible to execute arbitrary code as the user running Firefox if the user views a specially crafted Unicode sequence. (CVE-2005-2702)

A bug was found in the way Firefox makes XMLHttpRequest requests. It is possible that a malicious web page could leverage this flaw to exploit other proxy or server flaws from the victim's machine. It is also possible that this flaw could be leveraged to send XMLHttpRequest requests to hosts other than the originator; the default behavior of the browser is to disallow this. (CVE-2005-2703)

A bug was found in the way Firefox implemented its XBL interface. It may be possible for a malicious web page to create an XBL binding in such a way that would allow arbitrary JavaScript execution with chrome permissions. Please note that in Firefox 1.0.6 this issue is not directly exploitable and will need to leverage other unknown exploits. (CVE-2005-2704)

An integer overflow bug was found in Firefox's JavaScript engine. Under favorable conditions, it may be possible for a malicious web page to execute arbitrary code as the user running Firefox. (CVE-2005-2705)

A bug was found in the way Firefox displays about: pages. It

is possible for a malicious web page to open an about: page, such as about:mozilla, in such a way that it becomes possible to execute JavaScript with chrome privileges. (CVE-2005-2706)

A bug was found in the way Firefox opens new windows. It is possible for a malicious web site to construct a new window without any user interface components, such as the address bar and the status bar. This window could then be used to mislead the user for malicious purposes. (CVE-2005-2707)

A bug was found in the way Firefox processes URLs passed to it on the command line. If a user passes a malformed URL to Firefox, such as clicking on a link in an instant messaging program, it is possible to execute arbitrary commands as the user running Firefox. (CVE-2005-2968)

Users of Firefox are advised to upgrade to this updated package that contains Firefox version 1.0.7 and is not vulnerable to these issues.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2701](#), [CVE-2005-2702](#), [CVE-2005-2703](#), [CVE-2005-2704](#), [CVE-2005-2705](#), [CVE-2005-2706](#), [CVE-2005-2707](#), [CVE-2005-2968](#)

Nessus ID : [19876](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-598 (libtiff).

The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large.

The libtiff package should be installed if you need to manipulate TIFF format image files.

Update Information:

The updated libtiff package fixes an integer overflow which could lead to a buffer overflow in the tiffdump utility.

Solution : <http://www.fedoranews.org/blog/index.php?p=257>

Risk factor : High

Nessus ID : [16119](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-313 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

This update rebases the kernel to the latest upstream stable release, which fixes a number of security issues. Notably:

- CVE-2005-0210 : dst leak
- CVE-2005-0384 : ppp dos
- CVE-2005-0531 : Sign handling issues.
- CVE-2005-0400 : EXT2 information leak.
- CVE-2005-0449 : Remote oops.
- CVE-2005-0736 : Epoll overflow
- CVE-2005-0749 : ELF loader may kfree wrong memory.
- CVE-2005-0750 : Missing range checking in bluetooth
- CVE-2005-0767 : drm race in radeon
- CVE-2005-0815 : Corrupt isofs images could cause oops

Additionally, a large number of improvements have come from the 2.6.10 -> 2.6.11 transition.

This update requires you are running the latest udev package, and also (if you are using SELinux) the latest selinux policy packages.

* Thu Apr 7 2005 Dave Jones <davej redhat com>

- Update to 2.6.11.7
- Set CFQ as default elevator again.

* Tue Apr 5 2005 Dave Jones <davej redhat com>

- Disable slab debug.
- Re-add the pwc driver. (#152593)

* Wed Mar 30 2005 Dave Jones <davej redhat com>

- x86_64: Only free PMDs and PUDs after other CPUs have been flushed

- * Sat Mar 26 2005 Dave Jones <davej redhat com>
- Update to 2.6.11.6
- * Tue Mar 22 2005 Dave Jones <davej redhat com>
- Fix up several calls to memset with swapped arguments.
- * Sat Mar 19 2005 Dave Jones <davej redhat com>
- Update to 2.6.11.5
- * Fri Mar 18 2005 Dave Jones <davej redhat com>
- Kjournald oops race. (#146344)
- * Tue Mar 15 2005 Dave Jones <davej redhat com>
- Update to 2.6.11.4
- * Thu Mar 10 2005 Dave Jones <davej redhat com>
- Update to 2.6.11.2
- Reenable advansys driver for x86
- * Fri Mar 4 2005 Dave Jones <davej redhat com>
- Fix up ACPI vs keyboard controller problem.
- Fix up Altivec usage on PPC/PPC64.
- * Fri Mar 4 2005 Dave Jones <davej redhat com>
- Finger the programs that try to read from /dev/mem.
- Improve spinlock debugging a little.
- * Wed Mar 2 2005 Dave Jones <davej redhat com>
- 2.6.11

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0210](#), [CVE-2005-0384](#), [CVE-2005-0400](#), [CVE-2005-0449](#), [CVE-2005-0531](#), [CVE-2005-0736](#), [CVE-2005-0749](#), [CVE-2005-0750](#), [CVE-2005-0767](#), [CVE-2005-0815](#)

Nessus ID : [19648](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-562 (samba).

Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available

files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called 'Lan Manager') clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

* Fri Dec 17 2004 Jay Fenlason 3.0.10-1.fc3

- New upstream release that closes CVE-2004-1154 bz#142544
- Include the -64bit patch from Nalin. This closes bz#142873
- Update the -logfiles patch to work with 3.0.10
- Create /var/run/winbindd and make it part of the -common rpm to close bz#142242

Solution : <http://www.fedoranews.org/blog/index.php?p=216>

Risk factor : High

CVE : [CVE-2004-1154](#)

Nessus ID : [16027](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-319 (sharutils).

The sharutils package contains the GNU shar utilities, a set of tools for encoding and decoding packages of files (in binary or text format) in a special plain text format called shell archives (shar). This format can be sent through e-mail (which can be problematic for regular binary files). The shar utility supports a wide range of capabilities (compressing, uuencoding, splitting long files for multi-part mailings, providing checksums), which make it very flexible at creating shar files. After the files have been sent, the unshar tool scans mail messages looking for shar files. Unshar automatically strips off mail headers and introductory text and then unpacks the shar files.

Install sharutils if you send binary files through e-mail.

* Mon Apr 11 2005 Than Ngo <than redhat com> 4.2.1-22.2.FC3

- apply debian patch to fix insecure temporary file creation in unshar #154049, CVE-2005-0990

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0990](#)
Nessus ID : [19651](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-373 (squid).

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.

* Mon May 16 2005 Jay Fenlason 7:2.5.STABLE9-1.FC3.6

- More upstream patches, including ones for
bz#157456 CVE-2005-1519 DNS lookups unreliable on untrusted networks
bz#156162 CVE-1999-0710 cachemgr.cgi access control bypass

- The following bugs had already been fixed, but the announcements were lost
bz#156711 CVE-2005-1390 HTTP Request Smuggling Vulnerabilities
bz#156703 CVE-2005-1389 HTTP Response Splitting Vulnerabilities
(Both fixed by squid-7:2.5.STABLE8-1.FC3.1)
bz#151419 Unexpected access control results on configuration errors
(Fixed by 7:2.5.STABLE9-1.FC3.2)
bz#152647#squid-2.5.STABLE9-1.FC3.4.x86_64.rpm is broken
(fixed by 7:2.5.STABLE9-1.FC3.5)
bz#141938 squid ldap authentication broken
(Fixed by 7:2.5.STABLE7-1.FC3)

* Fri Apr 1 2005 Jay Fenlason 7:2.5.STABLE9-1.FC3.5

- More upstream patches, including a new version of the -2GB patch that doesn't break diskd.

Solution : <http://www.fedoranews.org/blog/index.php?p=681>
Risk factor : High
CVE : [CVE-2005-1389](#), [CVE-2005-1390](#), [CVE-2005-1519](#), [CVE-1999-0710](#)
Nessus ID : [18337](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-260 (squirrelmail).

SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.

Update Information:

Multiple issues in squirrelmail (CVE-2005-0104)
Upgrade to 1.4.4

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0104](#)
Nessus ID : [19638](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-421 (httpd).

Apache is a powerful, full-featured, efficient, and freely-available Web server. Apache is also the most popular Web server on the Internet.

Update Information:

This update includes the fix for a memory consumption denial of service issue in the handling of request header lines (CVE CVE-2004-0942).

Solution : <http://www.fedoranews.org/blog/index.php?p=72>

Risk factor : High

CVE : [CVE-2004-0942](#)

Nessus ID : [15735](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-985 (openssl096b).

The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.

* Thu Oct 6 2005 Tomas Mraz <tmraz redhat com> 0.9.6b-21.2
- fix CVE-2005-2969 - remove SSL_OP_MSIE_SSLV2_RSA_PADDING which disables the countermeasure against man in the middle attack in SSLv2 (#169863)
- more fixes for constant time/memory access for DSA signature algorithm
- replaced add-luna patch with new one with right license (#158061)

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2969](#)

Nessus ID : [20022](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-092 (enscript).

GNU enscript is a free replacement for Adobe's Enscript program. Enscript converts ASCII files to PostScript(TM) and spools generated PostScript output to the specified printer or saves it to a file. Enscript can be extended to handle different output media and includes many options for customizing printouts.

Update Information:

This update fixes a regression introduced by the last update.

Solution : <http://www.fedoranews.org/blog/index.php?p=340>

Risk factor : High

CVE : [CVE-2004-1184](#)

Nessus ID : [16287](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-344 (ImageMagick).

ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more.

ImageMagick is one of your choices if you need a program to manipulate and display images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.

Update Information:

The update fixes a possible heap corruption issue in the pnm decoder. It also includes a number of other bug fixes and improvements.

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19656](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-304 (mysql).

MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries.

* Sat Apr 2 2005 Tom Lane <tgl redhat com> 3.23.58-16.FC3.1

- Repair uninitialized variable in security2 patch.
- Enable testing on 64-bit arches; continue to exclude s390x which still has issues.

* Sat Mar 19 2005 Tom Lane <tgl redhat com> 3.23.58-15.FC3.1

- Backpatch repair for CVE-2005-0709, CVE-2005-0710, CVE-2005-0711 (bz#151051).
- Run 'make test' only on the archs we support for FC-3.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0711](#)

Nessus ID : [19646](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-281 (sharutils).

The sharutils package contains the GNU shar utilities, a set of tools for encoding and decoding packages of files (in binary or text format) in a special plain text format called shell archives (shar). This format can be sent through e-mail (which can be problematic for regular binary files). The shar utility supports a wide range of capabilities (compressing, uuencoding, splitting long files for multi-part mailings, providing checksums), which make it very flexible at creating shar files. After the files have been sent, the unshar tool scans mail messages looking for shar files. Unshar automatically strips off mail headers and introductory text and then unpacks the shar files.

Install sharutils if you send binary files through e-mail.

* Thu Mar 31 2005 Than Ngo <than redhat com> 4.2.1-22.1.FC3

- apply patch to fix multiple buffer overflows #152574

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19644](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-575 (cups).

The Common UNIX Printing System provides a portable printing layer for UNIX operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users.

CUPS provides the System V and Berkeley command-line interfaces.

Update Information:

This package fixes a buffer overflow which may possibly allow attackers to execute arbitrary code as the 'lp' user. The Common Vulnerabilities and Exposures projects (cve.mitre.org) has assigned the name CVE-2004-1125 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=227>
Risk factor : High
CVE : [CVE-2004-1125](#)
Nessus ID : [16052](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-600 (perl).

Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts.

Install this package if you want to program in Perl or enable your system to handle Perl scripts.

Update Information:

Paul Szabo discovered another vulnerability in the File::Path::rmtree function of perl, the popular scripting language. When a process is deleting a directory tree, a different user could exploit a race condition to create setuid binaries in this directory tree, provided that he already had write permissions in any subdirectory of that tree.

Perl interpreter would cause a segmentation fault when environment changes during the runtime.

Code in lib/FindBin contained a regression which caused problems with MRTG software package.

All of the above problems are now fixed in perl-5.8.5-14.FC3. Please test as much as you can and report any problems/regressions.

Solution : <http://www.fedoranews.org/blog/index.php?p=786>

Risk factor : High

CVE : [CVE-2005-0448](#)

Nessus ID : [19290](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-733 (cups).

The Common UNIX Printing System provides a portable printing layer for UNIX(R) operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.

Update Information:

These updated packages fix a problem handling PDF files that could have security implications (CVE-2005-2097).

Solution : <http://www.fedoranews.org/blog/index.php?p=848>
Risk factor : High
CVE : [CVE-2005-2097](#)
Nessus ID : [19468](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-160 (gaim).

Gaim allows you to talk to anyone using a variety of messaging protocols, including AIM (Oscar and TOC), ICQ, IRC, Yahoo!, MSN Messenger, Jabber, Gadu-Gadu, Napster, and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor.

Gaim supports many common features of other clients, as well as many unique features, such as perl scripting and C plugins.

Gaim is NOT affiliated with or endorsed by America Online, Inc., Microsoft Corporation, or Yahoo! Inc. or other messaging service providers.

* Sat Feb 19 2005 Warren Togami <wtogami redhat com> 1:1.1.3-1.FC3
- FC3

* Fri Feb 18 2005 Warren Togami <wtogami redhat com> 1:1.1.3-2
- 1.1.3 including two security fixes
CVE-2005-0472 Client freezes when receiving certain invalid messages
CVE-2005-0473 Client crashes when receiving specific malformed HTML

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0472](#), [CVE-2005-0473](#)
Nessus ID : [19619](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-133 (kdegraphics).

Graphics applications for the K Desktop Environment.

Includes:

kdvi (displays TeX .dvi files)
kfax (displays faxfiles)
kghostview (displays postscript files)
kcoloredit (palette editor and color chooser)
kamera (digital camera support)
kiconedit (icon editor)
kpaint (a simple drawing program)
ksnapshot (screen capture utility)
kview (image viewer for GIF, JPEG, TIFF, etc.)
kuickshow (quick picture viewer)
kooka (scanner application)
kruler (screen ruler and color measurement tool)

* Tue Feb 08 2005 Than Ngo
7:3.3.1-2.4

- More fixing of CVE-2004-0888 patch (bug #135393)

Solution : <http://www.fedoranews.org/blog/index.php?p=383>

Risk factor : High

CVE : [CVE-2004-0888](#)

Nessus ID : [16355](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-157 (postgresql).

PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions).

* Mon Feb 21 2005 Tom Lane <tgl@redhat.com> 7.4.7-3.FC3.1

- Work around selinux <<EOF problem during initdb (bug #149237).
- Repair improper error message in init script when PGVERSION doesn't match.
- Arrange for auto update of version embedded in init script.
- Fix improper call of strerror_r, which leads to junk error messages in libpq.
- Patch additional buffer overruns in plpgsql (CVE-2005-0247)

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0247](#)
Nessus ID : [19616](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-255 (evolution).

Evolution is the GNOME mailer, calendar, contact manager and communications tool. The tools which make up Evolution will be tightly integrated with one another and act as a seamless personal information-management tool.

Update Information:

There were several security flaws found in the mozilla package, which evolution depends on. Users of evolution are advised to upgrade to this updated package which has been rebuilt against a later version of mozilla which is not vulnerable to these flaws.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19637](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-821 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of the Red Hat Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

- * Fri Aug 26 2005 Dave Jones <davej redhat com> [2.6.12-1.1376_FC3]
- Better identify local builds. (#159696)
- Fix disk/net dump & netconsole. (#152586)
- Fix up sleeping in invalid context in sym2 driver. (#164995)
- Fix 'semaphore is not ready' error in snd-intel8x0m.
- Restore hwclock functionality on some systems. (#144894)

- Merge patches proposed for 2.6.12.6
 - Fix typo in ALPS driver.
 - Fix 'No sense' error with Transcend USB key. (#162559)
 - Fix up ide-scsi check for medium not present. (#160868)
 - powernow-k8 driver update from 2.6.13rc7
- * Tue Aug 23 2005 Dave Jones <davej redhat com> [2.6.12-1.1375_FC3]
 - Work around AMD x86-64 errata 122.
- * Thu Aug 18 2005 David Woodhouse <dwmw2 redhat com>
 - Don't probe 8250 ports on ppc32 unless they're in the device tree
 - Enable ISDN, 8250 console, i8042 keyboard controller on ppc32
 - Audit updates from git tree
- * Tue Aug 16 2005 Dave Jones <davej redhat com> [2.6.12-1.1374_FC3]
 - Restrict ipsec socket policy loading to CAP_NET_ADMIN. (CVE-2005-2555)
- * Mon Aug 15 2005 Dave Jones <davej redhat com>
 - 2.6.11.5
 - Fix module_verify_elf check that rejected valid .ko files. (#165528)
- * Thu Aug 11 2005 Dave Jones <davej redhat com>
 - Audit speedup in syscall path.
 - Update to a newer ACPI drop.
- * Wed Aug 10 2005 Dave Jones <davej redhat com>
 - Reenable 586-smp builds. (Another FC4 change that crept in).
- * Fri Aug 5 2005 Dave Jones <davej redhat com> [2.6.12-1.1373_FC3]
 - Sync with FC4 update.
 - Add Appletouch support.
 - Audit updates. In particular, don't printk audit messages that are passed from userspace when auditing is disabled.
 - update to final 2.6.12.4 patchset.
 - ACPI update to 20050729.
 - Disable experimental ACPI HOTKEY driver. (#163355)
- * Thu Aug 4 2005 Dave Jones <davej redhat com>
 - Enable Amiga partition support. (#149802)
- * Wed Aug 3 2005 Dave Jones <davej redhat com>
 - Silence some messages from PowerMac thermal driver. (#158739)
 - nfs server intermittently claimed ENOENT on existing files or directories. (#150759)
 - Stop usbhid driver incorrectly claiming Wireless Security Lock as a mouse. (#147479)
 - Further NFSD fixing for non-standard ports.
 - Fix up miscalculated i_nlink in /proc (#162418)

- Fix addrlen checks in selinux_socket_connect. (#164165)
- * Thu Jul 28 2005 Dave Jones <davej redhat com>
- Fix compilation with older gcc. (#164041)
- Bump mkinitrd minimum requirement.
- Drop the -devel changes that leaked in from the FC4 backport. (#163406)

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2555](#)

Nessus ID : [19723](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-564 (krb5).

Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.

A heap based buffer overflow bug was found in the administration library of Kerberos 1.3.5 and earlier. This overflow in the password history handling code could allow an authenticated remote attacker to execute commands on a realm's master Kerberos KDC. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-1189 to this issue.

Additionally a temporary file bug was found in the Kerberos krb5-send-pr command. It is possible that an attacker could create a specially crafted temporary file that could allow an arbitrary file to be overwritten which the victim has write access to. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-0971 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=219>

Risk factor : High

CVE : [CVE-2004-0642](#), [CVE-2004-0644](#), [CVE-2004-0772](#), [CVE-2004-0971](#), [CVE-2004-1189](#)

Nessus ID : [16029](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-274 (telnet).

Telnet is a popular protocol for logging into remote systems over the Internet. The telnet package provides a command line telnet client.

Update Information:

Two buffer overflow flaws were discovered in the way the telnet client handles messages from a server. An attacker may be able to execute arbitrary code on a victim's machine if the victim can be tricked into connecting to a malicious telnet server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CVE-2005-0468 and CVE-2005-0469 to these issues.

Red Hat would like to thank iDEFENSE for their responsible disclosure of this issue.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0468](#), [CVE-2005-0469](#)

Nessus ID : [19642](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-742 (evolution).

Evolution is the GNOME collection of personal information management (PIM) tools.

Evolution includes a mailer, calendar, contact manager and communication facility. The tools which make up Evolution will be tightly integrated with one another and act as a seamless personal information-management tool.

Update Information:

Fix for SITIC Vulnerability Advisory SA05-001

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19659](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-427 (spamassassin).

SpamAssassin provides you with a way to reduce if not completely eliminate

Unsolicited Commercial Email (SPAM) from your incoming email. It can be invoked by a MDA such as sendmail or postfix, or can be called from a procmail script, .forward file, etc. It uses a genetic-algorithm evolved scoring system to identify messages which look spammy, then adds headers to the message so they can be filtered by the user's mail reading software. This distribution includes the spamd/spamc components

which create a server that considerably speeds processing of mail.

To enable spamassassin, if you are receiving mail locally, simply add this line to your ~/.procmailrc:

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc
```

To filter spam for all users, add that line to /etc/procmailrc (creating if necessary).

Update Information:

Important update for a Denial of Service vulnerability, plus more bug fixes from upstream. More details available at:

<http://wiki.apache.org/spamassassin/NextRelease>

Solution : <http://www.fedoranews.org/blog/index.php?p=722>

Risk factor : High

CVE : [CVE-2005-1266](#)

Nessus ID : [18509](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-435 (ncpfs).

Ncpfs is a filesystem which understands the Novell NetWare(TM) NCP protocol. Functionally, NCP is used for NetWare the way NFS is used in the TCP/IP world. For a Linux system to mount a NetWare filesystem, it needs a special mount program. The ncpfs package

contains such a mount program plus other tools for configuring and using the ncpfs filesystem.

Install the ncpfs package if you need to use the ncpfs filesystem to use Novell NetWare files or services.

* Fri Jun 17 2005 Jiri Ryska 2.2.4-4.FC3.1

- fixed getuid security bug CVE-2005-0014
- fixed security bug CVE-2004-1079

* Mon Apr 11 2005 Jiri Ryska 2.2.4-4.FC3

- fixed getuid security bug CVE-2005-0013

Solution : <http://www.fedoranews.org/blog/index.php?p=843>

Risk factor : High

CVE : [CVE-2004-1079](#), [CVE-2005-0013](#), [CVE-2005-0014](#)

Nessus ID : [19464](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-874 (mozilla).

Mozilla is an open-source Web browser, designed for standards compliance, performance, and portability.

Update Information:

An updated mozilla package that fixes a security bug is now available for Fedora Core 3.

This update has been rated as having critical security impact by the Fedora Security Response Team.

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor.

A bug was found in the way Mozilla processes certain international domain names. An attacker could create a specially crafted HTML file, which when viewed by the victim would cause Mozilla to crash or possibly execute arbitrary code. The Common Vulnerabilities and Exposures project

(cve.mitre.org) has assigned the name CVE-2005-2871 to this issue.

Users of Mozilla are advised to upgrade to this updated package that contains a backported patch and is not vulnerable to this issue.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2871](#)

Nessus ID : [19736](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-252 (devhelp).

A API document browser for GNOME 2.

Update Information:

There were several security flaws found in the mozilla package, which devhelp depends on. Users of devhelp are advised to upgrade to this updated package which has been rebuilt against a later version of mozilla which is not vulnerable to these flaws.

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19635](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-933 (devhelp).

A API document browser for GNOME 2.

Update Information:

There were several security flaws found in the mozilla package, which devhelp depends on. Users of devhelp are advised to upgrade to this updated package which has been rebuilt against a version of mozilla not vulnerable to these

flaws.

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19878](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-247 (thunderbird).

Mozilla Thunderbird is a standalone mail and newsgroup client.

Update Information:

A buffer overflow bug was found in the way Thunderbird processes GIF images. It is possible for an attacker to create a specially crafted GIF image, which when viewed by a victim will execute arbitrary code as the victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0399 to this issue. A bug was found in the Thunderbird string handling functions. If a malicious website is able to exhaust a system's memory, it becomes possible to execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0255 to this issue.

Users of Thunderbird are advised to upgrade to this updated package which contains Thunderbird version 1.0.2 and is not vulnerable to these issues.

This update enables pango rendering by default.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0255](#), [CVE-2005-0399](#)

Nessus ID : [19633](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-116 (emacs).

Emacs is a powerful, customizable, self-documenting, modeless text editor. Emacs contains special code editing features, a scripting language (elisp), and the capability to read mail, news, and more without leaving the editor.

This package provides an emacs binary with support for X windows.

Update Information:

This update fixes the CVE-2005-0100 movemail vulnerability and backports the latest bug fixes.

Solution : <http://www.fedoranews.org/blog/index.php?p=380>

Risk factor : High

CVE : [CVE-2005-0100](#)

Nessus ID : [16350](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-367 (htdig).

The ht://Dig system is a complete world wide web indexing and searching system for a small domain or intranet. This system is not meant to replace the need for powerful internet-wide search systems like Lycos, Infoseek, Webcrawler and AltaVista. Instead it is meant to cover the search needs for a single company, campus, or even a particular sub section of a web site. As opposed to some WAIS-based or web-server based search engines, ht://Dig can span several web servers at a site. The type of these different web servers doesn't matter as long as they understand the HTTP 1.0 protocol. ht://Dig is also used by KDE to search KDE's HTML documentation.

ht://Dig was developed at San Diego State University as a way to search the various web servers on the campus network.

* Tue Apr 19 2005 Phil Knirsch <pknirsch redhat com> 3:3.2.0b6-3.FC3.1
- Fixed security bug with unescaped output in htsearch and qtest (#144127)
- Removed .la and .a libs from package (#145649)

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19658](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-934 (epiphany).

epiphany is a simple GNOME web browser based on the Mozilla rendering engine

Update Information:

There were several security flaws found in the mozilla package, which epiphany depends on. Users of epiphany are advised to upgrade to this updated package which has been rebuilt against a version of mozilla not vulnerable to these flaws.

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19879](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-962 (thunderbird).

Mozilla Thunderbird is a standalone mail and newsgroup client.

Update Information:

An updated thunderbird package that fixes various bugs is now available for Fedora Core 3.

This update has been rated as having important security impact by the Fedora Security Response Team.

Mozilla Thunderbird is a standalone mail and newsgroup client.

A bug was found in the way Thunderbird processes certain international domain names. An attacker could create a specially crafted HTML file, which when viewed by the victim would cause Thunderbird to crash or possibly execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2871 to this issue.

A bug was found in the way Thunderbird processes certain Unicode sequences. It may be possible to execute arbitrary code as the user running Thunderbird if the user views a

specially crafted Unicode sequence. (CVE-2005-2702)

A bug was found in the way Thunderbird makes XMLHttpRequest requests. It is possible that a malicious web page could leverage this flaw to exploit other proxy or server flaws from the victim's machine. It is also possible that this flaw could be leveraged to send XMLHttpRequest requests to hosts other than the originator; the default behavior of the browser is to disallow this. (CVE-2005-2703)

A bug was found in the way Thunderbird implemented its XBL interface. It may be possible for a malicious web page to create an XBL binding in such a way that would allow arbitrary JavaScript execution with chrome permissions. Please note that in Thunderbird 1.0.6 this issue is not directly exploitable and will need to leverage other unknown exploits. (CVE-2005-2704)

An integer overflow bug was found in Thunderbird's JavaScript engine. Under favorable conditions, it may be possible for a malicious mail message to execute arbitrary code as the user running Thunderbird. Please note that JavaScript support is disabled by default in Thunderbird. (CVE-2005-2705)

A bug was found in the way Thunderbird displays about: pages. It is possible for a malicious web page to open an about: page, such as about:mozilla, in such a way that it becomes possible to execute JavaScript with chrome privileges. (CVE-2005-2706)

A bug was found in the way Thunderbird opens new windows. It is possible for a malicious web site to construct a new window without any user interface components, such as the address bar and the status bar. This window could then be used to mislead the user for malicious purposes. (CVE-2005-2707)

A bug was found in the way Thunderbird processes URLs passed to it on the command line. If a user passes a malformed URL to Thunderbird, such as clicking on a link in an instant messaging program, it is possible to execute arbitrary commands as the user running Thunderbird. (CVE-2005-2968)

Users of Thunderbird are advised to upgrade to this updated package that contains Thunderbird version 1.0.7 and is not vulnerable to these issues.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2702](#), [CVE-2005-2703](#), [CVE-2005-2704](#), [CVE-2005-2705](#), [CVE-2005-2706](#), [CVE-2005-2707](#), [CVE-2005-2871](#), [CVE-2005-2968](#)

Nessus ID : [19883](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-406 (tcpdump).

Tcpdump is a command-line tool for monitoring network traffic. Tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria.

Install tcpdump if you need a program to monitor network traffic.

* Tue Jun 07 2005 Martin Stransky - 14:3.8.2-9.FC3

- fix for CVE-2005-1267 - BGP DoS, #159209

Solution : <http://www.fedoranews.org/blog/index.php?p=716>

Risk factor : High

CVE : [CVE-2005-1267](#)

Nessus ID : [18439](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-812 (ntp).

The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. The ntp package contains utilities and daemons that will synchronize your computer's time to Coordinated Universal Time (UTC) via the NTP protocol and NTP servers. The ntp package includes ntpdate (a program for retrieving the date and time from remote machines via a network) and ntpd (a daemon which continuously adjusts system time).

Install the ntp package if you need tools for keeping your system's time synchronized via the NTP protocol.

Update Information:

When starting xntpd with the -u option and specifying the group by using a string not a numeric gid the daemon uses the gid of the user not the group. This problem is now fixed by this update.

The Common Vulnerabilities and Exposures project assigned the name CVE-2005-2496 to this issue.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2496](#)

Nessus ID : [19720](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-245 (kdelibs).

Libraries for the K Desktop Environment:

KDE Libraries included: kdeccore (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kingio (image manipulation).

* Wed Mar 23 2005 Than Ngo <than redhat com> 6:3.3.1-2.9.FC3
- Applied patch to fix konqueror international domain name spoofing, CVE-2005-0237, #147405
- get rid of broken AltiVec instructions on ppc

* Wed Mar 2 2005 Than Ngo <than redhat com> 6:3.3.1-2.8.FC3
- Applied patch to fix DCOP DoS, CVE-2005-0396, #150092
thanks KDE security team

* Wed Feb 16 2005 Than Ngo <than redhat com> 6:3.3.1-2.7.FC3
- Applied patch to fix dcpidlng insecure temporary file usage, CVE-2005-0365, #148823

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0237](#), [CVE-2005-0365](#), [CVE-2005-0396](#)

Nessus ID : [19631](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-603 (firefox).

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Users of Firefox are advised to upgrade to this updated package that contains Firefox version 1.0.6 and is not vulnerable to these issues.

Solution : <http://www.fedoranews.org/blog/index.php?p=777>

Risk factor : High

Nessus ID : [19260](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-552 (krb5).

Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.

Update Information:

A double-free flaw was found in the `krb5_recvauth()` routine which may be triggered by a remote unauthenticated attacker. Fedora Core 3 contains checks within `glibc` that detect double-free flaws. Therefore, on Fedora Core 3, successful exploitation of this issue can only lead to a denial of service (KDC crash). The Common Vulnerabilities and Exposures project assigned the name CVE-2005-1689 to this issue.

Daniel Wachdorf discovered a single byte heap overflow in the `krb5_unparse_name()` function, part of `krb5-libs`. Successful exploitation of this flaw would lead to a denial of service (crash). To trigger this flaw remotely, an attacker would need to have control of a kerberos realm that shares a cross-realm key with the target, making exploitation of this flaw unlikely. (CVE-2005-1175).

Daniel Wachdorf also discovered that in error conditions that may occur in response to correctly-formatted client requests, the Kerberos 5 KDC may attempt to free uninitialized memory. This could allow a remote attacker to cause a denial of service (KDC crash) (CVE-2005-1174).

Ga l Delalleau discovered an information disclosure issue in the way

some telnet clients handle messages from a server. An attacker could construct a malicious telnet server that collects information from the environment of any victim who connects to it using the Kerberos-aware telnet client (CVE-2005-0488).

The rcp protocol allows a server to instruct a client to write to arbitrary files outside of the current directory. This could potentially cause a security issue if a user uses the Kerberos-aware rcp to copy files from a malicious server (CVE-2004-0175).

Solution : <http://www.fedoranews.org/blog/index.php?p=753>

Risk factor : High

CVE : [CVE-2004-0175](#), [CVE-2005-0488](#), [CVE-2005-1174](#), [CVE-2005-1175](#), [CVE-2005-1689](#)

Nessus ID : [18684](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-872 (firefox).

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

An updated firefox package that fixes as security bug is now available for Fedora Core 3 and Fedora Core 4.

This update has been rated as having critical security impact by the Fedora Security Response Team.

Mozilla Firefox is an open source Web browser.

A bug was found in the way Firefox processes certain international domain names. An attacker could create a specially crafted HTML file, which when viewed by the victim would cause Firefox to crash or possibly execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2871 to this issue.

Users of Firefox are advised to upgrade to this updated package that contains a backported patch and is not vulnerable to this issue.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2871](#)
Nessus ID : [19734](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-309 (gftp).

gFTP is a multi-threaded FTP client for the X Window System. gFTP supports simultaneous downloads, resumption of interrupted file transfers, file transfer queues to allow downloading of multiple files, support for downloading entire directories/subdirectories, a bookmarks menu to allow quick connection to FTP sites, caching of remote directory listings, local and remote chmod, drag and drop, a connection manager and much more.

Install gftp if you need a graphical FTP client.

- * Fri Feb 18 2005 Warren Togami <wtogami redhat com> 2.0.18-0.FC3
- FC3 (including CVE-2005-0372)
- * Thu Feb 10 2005 Warren Togami <wtogami redhat com> 2.0.18-1
- 2.0.18

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0372](#)
Nessus ID : [19647](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-932 (mozilla).

Mozilla is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

Updated mozilla packages that fix several security bugs are now available for Fedora Core 3.

This update has been rated as having critical security impact by the Fedora Security Response Team.

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor.

A bug was found in the way Mozilla processes XBM image files. If a user views a specially crafted XBM file, it becomes possible to execute arbitrary code as the user running Mozilla. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2701 to this issue.

A bug was found in the way Mozilla processes certain Unicode sequences. It may be possible to execute arbitrary code as the user running Mozilla, if the user views a specially crafted Unicode sequence. (CVE-2005-2702)

A bug was found in the way Mozilla makes XMLHttpRequests. It is possible that a malicious web page could leverage this flaw to exploit other proxy or server flaws from the victim's machine. It is also possible that this flaw could be leveraged to send XMLHttpRequests to hosts other than the originator; the default behavior of the browser is to disallow this. (CVE-2005-2703)

A bug was found in the way Mozilla implemented its XBL interface. It may be possible for a malicious web page to create an XBL binding in a way that would allow arbitrary JavaScript execution with chrome permissions. Please note that in Mozilla 1.7.10 this issue is not directly exploitable and would need to leverage other unknown exploits. (CVE-2005-2704)

An integer overflow bug was found in Mozilla's JavaScript engine. Under favorable conditions, it may be possible for a malicious web page to execute arbitrary code as the user running Mozilla. (CVE-2005-2705)

A bug was found in the way Mozilla displays about: pages. It is possible for a malicious web page to open an about: page, such as about:mozilla, in such a way that it becomes

possible to execute JavaScript with chrome privileges.
(CVE-2005-2706)

A bug was found in the way Mozilla opens new windows. It is possible for a malicious web site to construct a new window without any user interface components, such as the address bar and the status bar. This window could then be used to mislead the user for malicious purposes. (CVE-2005-2707)

Users of Mozilla are advised to upgrade to this updated package that contains Mozilla version 1.7.12 and is not vulnerable to these issues.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2701](#), [CVE-2005-2702](#), [CVE-2005-2703](#), [CVE-2005-2704](#), [CVE-2005-2705](#), [CVE-2005-2706](#), [CVE-2005-2707](#), [CVE-2005-2968](#)

Nessus ID : [19877](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-315 (php).

PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The mod_php module enables the Apache Web server to understand and process the embedded PHP language in Web pages.

Update Information:

This update includes the latest stable release of PHP 4.3, including a number of security fixes to the exif extension (CVE CVE-2005-1042 and CVE-2005-1043) and the getimagesize() function (CVE CVE-2005-0524), along with many bug fixes.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0524](#), [CVE-2005-1042](#)
Nessus ID : [19649](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-237 (xloadimage).

The xloadimage utility displays images in an X Window System window, loads images into the root window, or writes images into a file. Xloadimage supports many image types (including GIF, TIFF, JPEG, XPM, and XBM).

Update Information:

This update fixes CVE-2005-0638, a problem in the parsing of shell metacharacters in filenames. It also fixes bugs in handling of malformed TIFF and PBM/PNM/PPM issues.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0638](#)

Nessus ID : [19629](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-730 (xpdf).

Xpdf is an X Window System based viewer for Portable Document Format (PDF) files. Xpdf is a small and efficient program which uses standard X fonts.

Update Information:

A flaw was discovered in Xpdf in that an attacker could construct a carefully crafted PDF file that would cause Xpdf to consume all available disk space in /tmp when opened. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-2097 to this issue.

Users of xpdf should upgrade to this updated package, which contains a backported patch to resolve this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=838>

Risk factor : High

CVE : [CVE-2005-2097](#)

Nessus ID : [19435](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-268 (gtk2).

GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.

Update Information:

David Costanzo found a bug in the way GTK+ processes BMP images. It is possible that a specially crafted BMP image could cause a denial of service attack in applications linked against GTK+. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0891 to this issue.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0891](#)

Nessus ID : [19640](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-1030 (pam).

PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.

Update Information:

This update fixes a security bug in `unix_chkpwd` allowing brute force attacks against passwords in `/etc/shadow` by a regular user when SELinux is enabled.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CAN-2005-2977](#)
Nessus ID : [20098](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-815 (lesstif).

LessTif is a free replacement for OSF/Motif(R), which provides a full set of widgets for application development (menus, text entry areas, scrolling windows, etc.). LessTif is source compatible with OSF/Motif(R) 1.2. The widget set code is the primary focus of development. If you are installing lesstif, you also need to install lesstif-clients.

* Fri May 6 2005 Thomas Woerner <twoerner redhat com> 0.93-36-6.FC3.2
- fixed possible libXpm overflows (#151640)
- allow to write XPM files with absolute path names again (#140815)

* Fri Nov 26 2004 Thomas Woerner <twoerner redhat com> 0.93.36-6.FC3.1
- fixed CVE-2004-0687 (integer overflows) and CVE-2004-0688 (stack overflows) in embedded Xpm library (#135080)
- latest Xpm patches: CVE-2004-0914 (#135081)

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2004-0688](#), [CVE-2004-0914](#)
Nessus ID : [19721](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-604 (thunderbird).

Mozilla Thunderbird is a standalone mail and newsgroup client.

Users of Thunderbird are advised to upgrade to this updated package

that contains Thunderbird version 1.0.6 and is not vulnerable to these issues.

Solution : <http://www.fedoranews.org/blog/index.php?p=778>

Risk factor : High

CVE : [CVE-2005-0989](#), [CVE-2005-1159](#), [CVE-2005-1160](#), [CVE-2005-1532](#), [CVE-2005-2261](#), [CVE-2005-2265](#), [CVE-2005-2266](#), [CVE-2005-2269](#), [CVE-2005-2270](#)

Nessus ID : [19261](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-146 (xemacs).

XEmacs is a highly customizable open source text editor and application development system. It is protected under the GNU Public License and related to other versions of Emacs, in particular GNU Emacs. Its emphasis is on modern graphical user interface support and an open software development model, similar to Linux.

This package contains xemacs built for X Windows with MULE support.

Update Information:

Update to 21.4.17 stable release, which also fixes the CVE-2005-0100 movemail string format vulnerability and the AltGr issue for European input.

Solution : <http://www.fedoranews.org/blog/index.php?p=399>

Risk factor : High

CVE : [CVE-2005-0100](#)

Nessus ID : [16467](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-941 (HelixPlayer).

The Helix Player 1.0 is an open-source media player built in the Helix Community for consumers. Built using GTK, it plays open source formats, like Ogg Vorbis and Theora using the powerful Helix DNA Client Media Engine.

Update Information:

This is a fix for CVE-2005-2710

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2710](#)

Nessus ID : [19881](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-886 (util-linux).

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.

* Wed Sep 14 2005 Karel Zak <kzak redhat com> 2.12a-24.5
- fix #168207 - CVE-2005-2876 umount unsafe -r usage

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2876](#)

Nessus ID : [19737](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-460 (samba).

Samba is the protocol by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called 'Lan Manager') clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw

NetBIOS frame) protocol.

Update Information:

This update closes two security holes: CVE-2004-0882 and CVE-2004-0930.

Solution : <http://www.fedoranews.org/blog/index.php?p=124>

Risk factor : High

CVE : [CVE-2004-0882](#), [CVE-2004-0930](#)

Nessus ID : [15848](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-568 (php).

PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The mod_php module enables the Apache Web server to understand and process the embedded PHP language in Web pages.

This update includes the latest release of PHP 4.3, including fixes for security issues in the unserializer (CVE CVE-2004-1019) and exif image parsing (CVE CVE-2004-1065).

Solution : <http://www.fedoranews.org/blog/index.php?p=221>

Risk factor : High

CVE : [CVE-2004-1019](#), [CVE-2004-1065](#)

Nessus ID : [16031](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-338 (evolution).

Evolution is the GNOME mailer, calendar, contact manager and

communications tool. The tools which make up Evolution will be tightly integrated with one another and act as a seamless personal information-management tool.

* Fri Apr 22 2005 David Malcolm <dmalcolm redhat com> - 2.0.4-4

- Added the correct patch this time

* Wed Apr 20 2005 David Malcolm <dmalcolm redhat com> - 2.0.4-3

- Added patch for #155378 (CVE-2005-0806)

- Updated mozilla_build_version from 1.7.6 to 1.7.7

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0806](#)

Nessus ID : [19655](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-953 (w3c-libwww).

Libwww is a general-purpose Web API written in C for Unix and Windows (Win32). With a highly extensible and layered API, it can accommodate many different types of applications including clients, robots, etc. The purpose of libwww is to provide a highly optimized HTTP sample implementation as well as other Internet protocols and to serve as a testbed for protocol experiments.

Update Information:

This update fixes libwww's handling of multipart/byteranges content and a possible stack overflow.

Solution : Get the newest Fedora Updates

Risk factor : High

Nessus ID : [19972](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-474 (ruby).

Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.

* Wed Jun 22 2005 Akira TAGOH - 1.8.2-1.fc3.3

- ruby-1.8.2-xmlrpc-CVE-2005-1992.patch: fixed the arbitrary command execution on XMLRPC server. (#161096)

Solution : <http://www.fedoranews.org/blog/index.php?p=726>

Risk factor : High

CVE : [CVE-2005-1992](#)

Nessus ID : [18543](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-123 (cups).

The Common UNIX Printing System provides a portable printing layer for UNIX operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.

Update Information:

A problem with PDF handling was discovered by Chris Evans, and has been fixed. The Common Vulnerabilities and Exposures project (www.mitre.org) has assigned the name CVE-2004-0888 to this issue.

FEDORA-2004-337 attempted to correct this but the patch was incomplete.

Solution : <http://www.fedoranews.org/blog/index.php?p=377>

Risk factor : High

CVE : [CVE-2004-0888](#)
Nessus ID : [16352](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-738 (vim).

VIM (VIual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting and more.

Update Information:

CVE-2005-2368

Solution : <http://www.fedoranews.org/blog/index.php?p=814>

Risk factor : High

CVE : [CVE-2005-2368](#)

Nessus ID : [19421](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-893 (xorg-x11).

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality which full fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed upon.

Update Information:

Updated xorg-x11 packages that fix several integer overflows, various bugs, are now available for Fedora Core 3.

X.Org X11 is an implementation of the X Window System, which provides the core functionality for the Linux graphical desktop.

Several integer overflow bugs were found in the way X.Org X11 code parses pixmap images. It is possible for a user to gain elevated privileges by loading a specially crafted

pixmap image. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-2495 to this issue.

Additionally, this update contains:

- Support for some newer models of Intel i945 video chipsets.
- A change to the X server to make it use linux PCI config space access methods instead of directly touching the PCI config space registers itself. This prevents the X server from causing hardware lockups due accessing PCI config space at the same time the kernel has it locked. This is the latest revision of the PCI config space access patches, which fix a few regressions discovered on some hardware with previous patches.
- A fix for a memory leak in the X server's shadow framebuffer code.
- A problem with the Dutch keyboard layout has been resolved.
- The open source 'nv' driver for Nvidia hardware has been updated to the latest version. Additionally, a workaround has been added to the driver to disable known unstable acceleration primitives on some GeForce 6200/6600/6800 models.
- Several bugs have been fixed in the Xnest X server.
- DRI is now enabled by default on all ATI Radeon hardware except for the Radeon 7000/Radeon VE chipsets, which is known to be unstable for many users currently when DRI is enabled. Radeon 7000 users can re-enable DRI if desired by using Option 'DRI' in the device section of the config file, with the understanding that we consider it unstable currently.
- Added missing libFS.so and libGLw.so symlinks to the xorg-x11-devel package, which were inadvertently left out, causing apps to link to the static versions of these libraries.
- Fix xfs.init 'fonts.dir: No such file or directory' errors

A number of other issues have also been resolved. Please

consult the xorg-x11 rpm changelog for a detailed list.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-2495](#)

Nessus ID : [19739](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-1032 (gdb).

GDB, the GNU debugger, allows you to debug programs written in C, C++, and other languages, by executing them in a controlled fashion and printing their data.

Update Information:

This is an fc3 update for gdb regarding security issues:

CAN-2005-1704 Integer Overflow in gdb

This problem is that gdb's internal copy of bfd does not protect against heap-based overflow.

CAN-2005-1705 gdb arbitrary command execution

This problem allows unprotected .gdbinit files to execute arbitrary commands during gdb startup.

Fixes for both problems are found in:

`gdb-6.1post-1.20040607.43.0.1`

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CAN-2005-1704](#), [CAN-2005-1705](#)

Nessus ID : [20100](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-779 (squirrelmail).

SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.

Update Information:

It probably is not a good idea to push a CVS snapshot here, but upstream screwed up their 1.4.5 release and CVS contains further fixes like PHP5 related stuff that might make squirrelmail usable on FC4. This snapshot worked on my personal server for the past week, so hopefully it will be good for everyone else too.

CVE-2005-1769 and CVE-2005-2095 security issues are solved in this update.

Please report regressions in behavior from our previous 1.4.4 package to Red Hat Bugzilla, product Fedora Core. All other squirrelmail bugs please report upstream.

Solution : <http://www.fedoranews.org/blog/index.php?p=853>

Risk factor : High

CVE : [CVE-2005-2095](#)

Nessus ID : [19482](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-594 (kdelibs).

Libraries for the K Desktop Environment.

KDE Libraries include: kdecopre (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kimgio (image manipulation).

Update Information:

A flaw was discovered affecting Kate, the KDE advanced text editor, and Kwrite. Depending on system settings it may be possible for a local user to read the backup files created by Kate or Kwrite. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-1920 to this issue.

Users of Kate or Kwrite should update to this erratum package which contains a backported patch from the KDE security team correcting this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=776>

Risk factor : High

CVE : [CVE-2005-1046](#), [CVE-2005-1920](#)

Nessus ID : [19230](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-996 (wget).

GNU Wget is a file retrieval utility which can use either the HTTP or FTP protocols. Wget features include the ability to work in the background while you are logged out, recursive retrieval of directories, file name wildcard matching, remote file timestamp storage and comparison, use of Rest with FTP servers and Range with HTTP servers to retrieve files over slow or unstable connections, support for Proxy servers, and configurability.

Update Information:

This package fixes a buffer overflow bug in the NTLM authentication code of wget (CVE-2005-3185).

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-3185](#)

Nessus ID : [20029](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-517 (php).

PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The mod_php module enables the Apache Web server to understand and process the embedded PHP language in Web pages.

Update Information:

This update includes the PEAR XML_RPC 1.3.1 package, which fixes a security issue in the XML_RPC server implementation. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-1921 to this issue.

The bundled version of shtool is also updated, to fix some temporary file handling races. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-1751 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=739>

Risk factor : High

CVE : [CVE-2005-1751](#), [CVE-2005-1921](#)

Nessus ID : [18624](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-484 (HelixPlayer).

The Helix Player 1.0 is an open-source media player built in the Helix Community for consumers. Built using GTK, it plays open source formats, like Ogg Vorbis and Theora using the powerful Helix DNA Client Media Engine.

* Fri Jun 24 2005 Colin Walters 1:1.0.5-0.fc3.2

- Work done by John (J5) Palmieri

- Update to 1.0.5 as fix for bug #159872

Solution : <http://www.fedoranews.org/blog/index.php?p=729>

Risk factor : High

Nessus ID : [18582](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-235 (ImageMagick).

ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more.

ImageMagick is one of your choices if you need a program to manipulate and display images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.

Update Information:

Andrei Nigmatulin discovered a heap based buffer overflow flaw in the ImageMagick image handler. An attacker could create a carefully crafted Photoshop Document (PSD) image in such a way that it would cause ImageMagick to execute arbitrary code when processing the image. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0005 to this issue.

A format string bug was found in the way ImageMagick handles filenames. An attacker could execute arbitrary code in a victims machine if they are able to trick the victim into opening a file with a specially crafted name. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0397 to this issue.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0005](#), [CVE-2005-0397](#)

Nessus ID : [19628](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-1000 (curl).

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.

Update Information:

This package fixes a buffer overflow bug in NTLM authentication code of curl (CVE-2005-3185).

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-3185](#)

Nessus ID : [20056](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-188 (HelixPlayer).

The Helix Player 1.0 is an open-source media player built in the Helix Community for consumers. Built using GTK, it plays open source formats, like Ogg Vorbis and Theora using the powerful Helix DNA Client Media Engine.

Update Information:

Updated HelixPlayer packages that fixes two buffer overflow issues are now available.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

A stack based buffer overflow bug was found in HelixPlayer's Synchronized Multimedia Integration Language (SMIL) file processor. An attacker could create a specially crafted SMIL file which would execute arbitrary code when opened by a user. The Common Vulnerabilities and

Exposures project (cve.mitre.org) has assigned the name CVE-2005-0455 to this issue.

A buffer overflow bug was found in the way HelixPlayer decodes WAV files. An attacker could create a specially crafted WAV file which could execute arbitrary code when opened by a user. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-0611 to this issue.

All users of HelixPlayer are advised to upgrade to this updated package, which contains HelixPlayer 1.0.3 which is not vulnerable to these issues.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-0455](#), [CVE-2005-0611](#)
Nessus ID : [19623](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-616 (mozilla).

Mozilla is an open-source Web browser, designed for standards compliance, performance, and portability.

Users of Mozilla are advised to upgrade to these updated packages, which contain Mozilla version 1.7.10 and are not vulnerable to these issues.

Solution : <http://www.fedoranews.org/blog/index.php?p=781>
Risk factor : High
Nessus ID : [19273](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-577 (libtiff).

The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large.

The libtiff package should be installed if you need to manipulate TIFF format image files.

Update Information:

Fix several buffer overflow problems that could be used as an exploit.
Fixes the following security advisory: CVE-2004-1308

Solution : <http://www.fedoranews.org/blog/index.php?p=226>

Risk factor : High

CVE : [CVE-2004-1308](#)

Nessus ID : [16033](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-551 (kdebase).

Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).

* Tue Dec 14 2004 Than Ngo
6:3.3.1-4.3.FC3

- apply the patch to fix Konqueror Window Injection Vulnerability #142510
CVE-2004-1158, Thanks to KDE security team

* Fri Dec 10 2004 Than Ngo
6:3.3.1-4.2.FC3

- Security Advisory: plain text password exposure, thanks to KDE security team
- the existing icon is lost, add patch to fix this problem #140196
- add patch to fix kfind hang on search #137582
- rebuild against samba-3.0.9 #139894
- add CVS patch to fix konqueror crash by dragging some text over the navigation panel

- fix rpm conflict
- apply patch number 86
- add patch to fix man page problem konqueror, thanks to Andy Shevchenko

Solution : <http://www.fedoranews.org/blog/index.php?p=201>
Risk factor : High
CVE : [CVE-2004-1158](#)
Nessus ID : [15980](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-745 (kdeedu).

Educational/Edutainment applications for KDE

Update Information:

Ben Burton notified the KDE security team about several tempfile handling related vulnerabilities in langgen2kvtml, a conversion script for kvoctrain. The script must be manually invoked.

The script uses known filenames in /tmp which allow an local attacker to overwrite files writeable by the user invoking the conversion script.

This update fixes these vulnerabilities.

Solution : <http://www.fedoranews.org/blog/index.php?p=840>
Risk factor : High
CVE : [CVE-2005-2101](#)
Nessus ID : [19438](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-434 (xorg-x11).

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality which full fledged graphical user interfaces (GUIs) such as GNOME and KDE are designed

upon.

Update Information:

Several integer overflow flaws in the X.Org libXpm library used to decode XPM (X PixMap) images have been found and addressed. An attacker could create a carefully crafted XPM file which would cause an application to crash or potentially execute arbitrary code if opened by a victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2004-0914 to this issue.

Users are advised to upgrade to these erratum packages, which contain backported security patches as well as other bug fixes.

Solution : <http://www.fedoranews.org/blog/index.php?p=95>

Risk factor : High

CVE : [CVE-2004-0914](http://cve.mitre.org/cve/2004/0914)

Nessus ID : [15748](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-852 (squid).

Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.

- * Tue Sep 6 2005 Martin Stransky <stransky@redhat.com> 7:2.5.STABLE9-1.FC3.7
- Three upstream patches for #167414
- Spanish and Greek messages
- patch for -D_FORTIFY_SOURCE=2

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19730](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-984 (koffice).

The koffice package contains the KOffice office-type applications for the K Desktop Environment (KDE) GUI desktop. KOffice contains KWord, a word processor; KSpread, a spreadsheet; KPresenter, for presentations; and KChart, a diagram generator.

* Tue Oct 11 2005 Than Ngo <than redhat com> 4:1.4.2-0.FC3.2
- remove security fix which is included in new 1.4.2 upstream

* Thu Sep 29 2005 Than Ngo <than redhat com> 4:1.4.2-0.FC3.1
- update to 1.4.2
- apply upstream patch to fix CVE-2005-2971 kword buffer overflow #169486

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2971](#)
Nessus ID : [20021](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-989 (abiword).

AbiWord is a cross-platform Open Source word processor. The goal is to make AbiWord full-featured, and remain lean.

Update Information:

CVE-2005-2972 abiword multiple buffer overflows

Solution : Get the newest Fedora Updates
Risk factor : High

CVE : [CVE-2005-2972](#)
Nessus ID : [20024](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-016 (enscript).

GNU enscript is a free replacement for Adobe's Enscript program. Enscript converts ASCII files to PostScript(TM) and spools generated PostScript output to the specified printer or saves it to a file. Enscript can be extended to handle different output media and includes many options for customizing printouts.

Update Information:

Erik Sjlund has discovered several security relevant problems in enscript, a program to converts ASCII text to Postscript and other formats. The Common Vulnerabilities and Exposures project identifies the following vulnerabilities:

CVE-2004-1184

Unsanitised input can causes the execution of arbitrary commands via EPSF pipe support. This has been disabled, also upstream.

CVE-2004-1185

Due to missing sanitising of filenames it is possible that a specially crafted filename can cause arbitrary commands to be executed.

CVE-2004-1186

Multiple buffer overflows can cause the program to crash.

Solution : <http://www.fedoranews.org/blog/index.php?p=326>
Risk factor : High
CVE : [CVE-2004-1184](#), [CVE-2004-1185](#), [CVE-2004-1186](#)
Nessus ID : [16268](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-111 (dbus).

D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.

Update Information:

Security fix for Bug#146765 (CVE-2005-0201)

Solution : <http://www.fedoranews.org/blog/index.php?p=364>

Risk factor : High

CVE : [CVE-2005-0201](#)

Nessus ID : [16301](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-217 (ipsec-tools).

This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds:

- setkey, a program to directly manipulate policies and SAs
- racoon, an IKEv1 keying daemon

Update Information:

This update fixes a potential DoS in parsing ISAKMP headers in racoon. (CVE-2005-0398)

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-0398](#)

Nessus ID : [19627](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-981 (xloadimage).

The xloadimage utility displays images in an X Window System window, loads images into the root window, or writes images into a file. Xloadimage supports many image types (including GIF, TIFF, JPEG, XPM, and XBM).

* Mon Oct 10 2005 Martin Stransky <stransky redhat com> 4.1-35
- fix for CVE-2005-3178 xloadimage NIFF buffer overflow (#170150)

* Mon Apr 11 2005 Martin Stransky <stransky redhat com>
- fix a memory leak

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CVE-2005-3178](#)

Nessus ID : [19973](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-808 (openmotif).

This is the Open Motif 2.2.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager 'mwm'.

* Mon Apr 4 2005 Thomas Woerner <twoerner redhat com> 2.2.3-9.FC3.1
- fixed possible libXpm overflows (#151642)
- Upstream Fix: Multiscreen mode
- Upstream Fix: Crash when restarting by a session manager (motifzone#1193)
- Upstream Fix: Crash when duplicating a window menu containing f.circle_up (motifzone#1202)
- fixed divide by zero error in ComputeVizCount() (#144420)
- Xpmcreate: define LONG64 on 64 bit architectures (#143689)

* Mon Nov 29 2004 Thomas Woerner <twoerner redhat com> 2.2.3-6.FC3.2
- allow to write XPM files with absolute path names again (#140815)

Solution : Get the newest Fedora Updates

Risk factor : High
Nessus ID : [19666](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-320 (vixie-cron).

The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times. Vixie cron adds better security and more powerful configuration options to the standard version of cron.

- o Fixes security vulnerability CVE-2005-1038
([[14](http://www.securityfocus.com/archive/1/395093)])
- o Makes filename and command line length constraints correspond to system limits
- o Improved PAM support

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-1038](#)
Nessus ID : [19652](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-1008 (ethereal).

Ethereal is a network traffic analyzer for Unix-ish operating systems.

This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for ethereal. A graphical user interface is packaged separately to GTK+ package.

Update Information:

Ethereal 0.10.13 is scheduled to be released, which fixes the following issues:

The ISAKMP dissector could exhaust system memory.
(CAN-2005-3241)
Fixed in: r15163
Bug IDs: none
Versions affected: 0.10.11 to 0.10.12.

The FC-FCS dissector could exhaust system memory.
(CAN-2005-3241)
Fixed in: r15204
Bug IDs: 312
Versions affected: 0.9.0 to 0.10.12.

The RSVP dissector could exhaust system memory.
(CAN-2005-3241)
Fixed in: r15206, r15600
Bug IDs: 311, 314, 382
Versions affected: 0.9.4 to 0.10.12.

The ISIS LSP dissector could exhaust system memory.
(CAN-2005-3241)
Fixed in: r15245
Bug IDs: 320, 326
Versions affected: 0.8.18 to 0.10.12.

The IrDA dissector could crash. (CAN-2005-3242)
Fixed in: r15265, r15267
Bug IDs: 328, 329, 330, 334, 335, 336
Versions affected: 0.10.0 to 0.10.12.

The SLIMP3 dissector could overflow a buffer. (CAN-2005-3243)
Fixed in: r15279
Bug IDs: 327
Versions affected: 0.9.1 to 0.10.12.

The BER dissector was susceptible to an infinite loop.
(CAN-2005-3244)
Fixed in: r15292
Bug IDs: none
Versions affected: 0.10.3 to 0.10.12.

The SCSI dissector could dereference a null pointer and
crash. (CAN-2005-3246)
Fixed in: r15289
Bug IDs: none
Versions affected: 0.10.3 to 0.10.12.

If the 'Dissect unknown RPC program numbers' option was
enabled,

the ONC RPC dissector might be able to exhaust system memory.
This option is disabled by default. (CAN-2005-3245)
Fixed in: r15290
Bug IDs: none
Versions affected: 0.7.7 to 0.10.12.

The sFlow dissector could dereference a null pointer and crash (CAN-2005-3246)
Fixed in: r15375
Bug IDs: 356
Versions affected: 0.9.14 to 0.10.12.

The RTnet dissector could dereference a null pointer and crash (CAN-2005-3246)
Fixed in: r15673
Bug IDs: none
Versions affected: 0.10.8 to 0.10.12.

The SigComp UDVM could go into an infinite loop or crash. (CAN-2005-3247)
Fixed in: r15715, r15901, r15919
Bug IDs: none
Versions affected: 0.10.12.

If SMB transaction payload reassembly is enabled the SMB dissector could crash. This preference is disabled by default. (CAN-2005-3242)
Fixed in: r15789
Bug IDs: 421
Versions affected: 0.9.7 to 0.10.12.

The X11 dissector could attempt to divide by zero. (CAN-2005-3248)
Fixed in: r15927
Bug IDs: none
Versions affected: 0.10.1 to 0.10.12.

The AgentX dissector could overflow a buffer. (CAN-2005-3243)
Fixed in: r16003
Bug IDs: none
Versions affected: 0.10.10 to 0.10.12.

The WSP dissector could free an invalid pointer. (CAN-2005-3249)
Fixed in: r16220
Bug IDs: none
Versions affected: 0.10.1 to 0.10.12.

iDEFENSE found a buffer overflow in the SRVLOC dissector.
(CAN-2005-3184)
Fixed in: r16206
Bug IDs: none
Versions affected: 0.10.0 to 0.10.12.

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CAN-2005-3184](#), [CAN-2005-3241](#), [CAN-2005-3242](#), [CAN-2005-3243](#), [CAN-2005-3244](#), [CAN-2005-3245](#), [CAN-2005-3246](#), [CAN-2005-3247](#), [CAN-2005-3248](#), [CAN-2005-3249](#)
Nessus ID : [20074](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-487 (cyrus-imapd).

The cyrus-imapd package contains the core of the Cyrus IMAP server. It is a scaleable enterprise mail system designed for use from small to large enterprise environments using standards-based internet mail technologies.

A full Cyrus IMAP implementation allows a seamless mail and bulletin board environment to be set up across multiple servers. It differs from other IMAP server implementations in that it is run on 'sealed' servers, where users are not normally permitted to log in. The mailbox database is stored in parts of the filesystem that are private to the Cyrus IMAP server. All user access to mail is through software using the IMAP, POP3, or KPOP protocols. TLSv1 and SSL are supported for security.

Update Information:

Fix several buffer overflow problems that could be used as an exploit.
Fixes the following security advisories:
CVE-2004-1011 CVE-2004-1012 CVE-2004-1013 CVE-2004-1015

Solution : <http://www.fedoranews.org/blog/index.php?p=139>
Risk factor : High
CVE : [CVE-2004-1013](#), [CVE-2004-1015](#)
Nessus ID : [15895](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-562 (net-snmp).

SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmpttrapd daemons, documentation, etc.

You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities.

Building option:

-without tcp_wrappers : disable tcp_wrappers support

* Wed Jul 13 2005 Radek Vokal

- CVE-2005-2177 new upstream version fixing DoS (#162908)
- CVE-2005-1740 net-snmp insecure temporary file usage (#158770)
- session free fixed, agentx modules build fine (#157851)
- report gigabit Ethernet speeds using Ethtool (#152480)

Solution : <http://www.fedoranews.org/blog/index.php?p=755>

Risk factor : High

CVE : [CVE-2005-1740](#), [CVE-2005-2177](#)

Nessus ID : [19197](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-750 (gaim).

Gaim is a clone of America Online's Instant Messenger client. It features nearly all of the functionality of the official AIM client while also being smaller, faster, and commercial-free.

Update Information:

<http://gaim.sourceforge.net/>

Please see the Changelog details and security information at

the upstream Gaim Project site.

Solution : <http://www.fedoranews.org/blog/index.php?p=844>

Risk factor : High

CVE : [CVE-2005-2102](#), [CVE-2005-2103](#), [CVE-2005-2370](#)

Nessus ID : [19470](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-1007 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

Update Information:

This update fixes the outstanding kernel security issues for FC3, and fixes a number of regressions in the previous update kernel.

Solution : Get the newest Fedora Updates

Risk factor : High

CVE : [CAN-2005-2973](#), [CAN-2005-3179](#), [CAN-2005-3180](#), [CAN-2005-3181](#)

Nessus ID : [20073](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-623 (kdenetwork).

Networking applications for the K Desktop Environment.

Update Information:

Multiple integer overflow flaws were found in the way Kopete processes Gadu-Gadu messages. A remote attacker could send a specially crafted Gadu-Gadu message which would cause Kopete to crash or possibly execute arbitrary code. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-1852 to this issue.

Users of Kopete should update to these packages which contain a patch to correct this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=785>

Risk factor : High

CVE : [CVE-2005-1852](#)

Nessus ID : [19291](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-614 (fetchmail).

Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections. Fetchmail supports every remote-mail protocol currently in use on the Internet (POP2, POP3, RPOP, APOP, KPOP, all IMAPs, ESMTP ETRN, IPv6, and IPSEC) for retrieval. Then Fetchmail forwards the mail through SMTP so you can read it through your favorite mail client.

Install fetchmail if you need to retrieve mail over SLIP or PPP connections.

Update Information:

A buffer overflow was discovered in fetchmail's POP3 client. A malicious server could cause fetchmail to execute arbitrary code.

The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2355 to this issue.

All fetchmail users should upgrade to the updated package, which fixes this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=780>

Risk factor : High

CVE : [CVE-2005-2355](#)

Nessus ID : [19272](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-395 (ImageMagick).

ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more.

ImageMagick is one of your choices if you need a program to manipulate and display images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.

Update Information:

An malicious image could cause a denial-of-service in the xwd coder. The update fixes this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=699>

Risk factor : High

CVE : [CVE-2005-1739](#)

Nessus ID : [18378](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2004-585 (tetex).

TeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly.

Install tetex if you want to use the TeX text formatting system. If you are installing tetex, you will also need to install tetex-afm (a PostScript(TM) font converter for TeX), tetex-dvips (for converting .dvi files to PostScript format for printing on PostScript printers), tetex-latex (a higher level

formatting package which provides an easier-to-use interface for TeX), and tetex-xdvi (for previewing .dvi files in X). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.

Update Information:

The updated tetex package fixes a buffer overflow which allows attackers to cause the internal xpdf library used by applications in tetex to crash, and possibly to execute arbitrary code. The Common Vulnerabilities and Exposures projects (cve.mitre.org) has assigned the name CVE-2004-1125 to this issue.

Solution : <http://www.fedoranews.org/blog/index.php?p=235>

Risk factor : High

CVE : [CVE-2004-1125](http://cve.mitre.org/cve/2004/1125)

Nessus ID : [16099](https://www.tenable.com/plugins/nessus/16099)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-905 (kernel).

The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.

* Wed Sep 14 2005 Dave Jones <davej redhat com> [2.6.12-1.1378_FC3]
- Fixes for CVE-2005-2490 and CVE-2005-2492

* Mon Sep 5 2005 Dave Jones <davej redhat com>
- Fix aic7xxx issue with >4GB. (#167049)

* Fri Sep 2 2005 Dave Jones <davej redhat com> [2.6.12-1.1377_FC3]
- Various post 2.6.13 ACPI updates. (20050902)

* Mon Aug 29 2005 Dave Jones <davej redhat com>
- Fix local builds when '-' is in the hostname.
- Update ALPS driver to 2.6.13 level

Solution : Get the newest Fedora Updates
Risk factor : High
CVE : [CVE-2005-2492](#)
Nessus ID : [19868](#)

Vulnerability found on port general/tcp

The remote host is missing the patch for the advisory FEDORA-2005-182 (firefox).

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Update Information:

This update fixes several security vulnerabilities in Firefox 1.0.
It is recommended that all users update to Firefox 1.0.1.

Additionally, this update backports several fixes from rawhide.
This update enables pango font rendering by default.
This update enables smooth scrolling by default. On slower machines, this may cause scrolling to lag. If this is the case for you, you may disable smooth scrolling by going to Edit>Preferences>Advanced and uncheck 'Use smooth scrolling'.
This update also fixes the issue with downloads going to the user's home directory instead of the desktop, as expected.
See full changelog below for more.

Solution : Get the newest Fedora Updates
Risk factor : High
Nessus ID : [19622](#)

Information found on port general/tcp

HTTP NIDS evasion functions are enabled.
You may get some false negative results
Nessus ID : [10890](#)

Information found on port general/tcp

127.0.0.1 resolves as localhost.
Nessus ID : [12053](#)

Information found on port general/tcp

The output of "uname -a" is :
Linux machinename 2.6.9-1.667 #1 Tue Nov 2 14:41:25 EST 2004 i686 i686 i386
GNU/Linux

The remote Fedora system is :
Fedora Core release 3 (Heidelberg)

Local security checks have been enabled for this host.
Nessus ID : [12634](#)

Information found on port general/tcp

Using the remote HTTP banner, it is possible to guess that the
Linux distribution installed on the remote host is :
- Fedora Core 3
Nessus ID : [18261](#)

Information found on port general/tcp

Information about this scan :

Nessus version : 2.2.6
Plugin feed version : 200511080815
Type of plugin feed : Registered (7 days delay)
Scanner IP : 127.0.0.1
Port scanner(s) : nmap synscan netstat nessus_tcp_scanner
Port range : default
Thorough tests : yes
Experimental tests : yes
Paranoia level : 1
Report Verbosity : 2
Safe checks : no
Scan Start Date : 2005/12/2 18:54
Scan duration : 2255 sec

Nessus ID : [19506](#)

This file was generated by [Nessus](#), the open-sourced security scanner.

Bibliography

Amos Latteier, et al. The Zope Book: Ch. 19 Virtual Hosting Services. 2.6 Edition. Zope Community. Book. http://www.zope.org/Documentation/Books/ZopeBook/2_6Edition/ZopeBook-2_6.pdf.

Apacheweek. Feature: Using Virtual Hosts. Apacheweek. Web article. September 1996. <http://www.apacheweek.com/features/vhost>.

Dyer, Russell. Simplify Your Life with Apache Virtual Hosts. O'Reilly OnLAMP. Web article. July 2003. <http://www.onlamp.com/pub/a/apache/2003/07/24/vhosts.html>.

McKay, Andy. The Definitive Guide to Plone. First Edition. Enfold Systems. Book. May 2005. http://plone.org/documentation/manual/definitive-guide/definitive_guide_to_plone.pdf.

Springsteen, Joanna, Martin Aspeli. Plone End User Manual. Plone Community. User manual. February 2006. <http://plone.org/documentation/manual/end-user-manual/referencemanual-all-pages>.

List of symbols/abbreviations/acronyms/initialisms

ARMADA	Applied Research for MAritime Domain Awareness
CF	Canadian Forces
CLI	Command Line Interface
CMS	Content Management System
CNET	Classified Network
CSV	Comma Separated Value
DHCP	Dynamic Host Control Protocol
DN	Distinguished Name
DNS	Domain Name Service
DRDC	Defence Research Development Canada
DWAN	Defense Wide Area Network
FC3	Fedora Core 3
FTP	File Transfer Protocol
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
IP	Internet Protocol
KMSG	Knowledge Management Systems Group
MB	Megabyte
MS	Microsoft
MSOC	Marine Security Operation Centres
PDF	Portable Document Format
R&D	Research & Development
RAM	Random Access Memory
RFC	Request for Comment
RPM	Red Hat Package Manager
RSH	Remote Shell
SELinux	Security Enhanced Linux
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TTCP	The Technical Cooperation Program

URL	Uniform Resource Locator
WebDAV	Web-based Distributed Authoring and Versioning
WMF	Windows Metafile
Xinetd	Extended Internet Super Daemon
ZMI	Zope Management Interface
Zope	Z Object Publishing Environment

Glossary

Apache

Apache is an open source Web server that is available on most operating systems. It is with many other commercial applications including commercial database applications. It is by far currently the world's most popular Web server.

Certificate

A digital security, generally based on a public key encryption mechanism, is often used to both secure the network channel and verify the identity of a remote system.

CSV (Comma Separated Value)

CSV is generally a text-based file format where data is found entered into fields and the fields are delimited by a comma (.). CSV is a very common text file data format.

DHCP (Dynamic Host Control Protocol)

The Dynamic Host Configuration Protocol is a protocol used to dynamically assign a requesting client system all of the TCP/IP and networking configuration parameters it requires in order to correctly function on the network, such as IP address, gateway, netmask, DNS information, etc. It is defined in RFC 2131.

DNS (Domain Name Service)

The Domain Name System is a protocol used to perform name-to-IP-address (or the reverse) lookups. DNS converts machine names to their respective IP addresses and returns this information to a requesting client. It is defined in multiple RFC's.

Firewall

A firewall, either hardware and/or software is a system that implements a series of rules or security policies to enforce network behaviour on traffic passing through the networks connected to it. They are often found in conjunction with NAT-based systems or are themselves NAT-enabled. Firewalls are generally used when one wants to connect an internal network to one or more untrusted external networks such as the Internet.

Gateway

A gateway is generally an entry point into another network. The address denoted by the gateway often means the system is a router or is routing-capable. Gateways can often provide services such as NAT, firewalling, or translation (i.e. PC-to-mainframe gateway).

HTTP (Hypertext Transfer Protocol)

The Hypertext Transfer Protocol is a set of established rules which most Web browsers support to varying degrees that allows for the exchange of files and information (i.e. text, video, sound, multimedia, graphics, etc.) across the Internet and other TCP/IP-based

networks. It is also the standard protocol used for transmitting Web pages. HTTP 1.1 is defined by RFC 2616.

HTTPS (Hypertext Transfer Protocol over SSL)

HTTPS is HTTP over a secure, encrypted tunnel provided by SSL. Instead of running on port 80, it uses port 443. It is defined in RFC 2616.

IP (Internet Protocol) Address/Configuration

An IP Address is a computer-based address for communicating via the TCP/IP protocol stack. This address consists of four numbers separated by dots (.). Each number can range from 1 – 255. These addresses enable a computer-based system to connect and interoperate with other systems on a computer network, including but not limited to the Internet. An IP Configuration includes information such as IP address, gateway, and netmask.

Linux

Linux is a free and open source software operating system based on UNIX. It was originally conceived and developed (the kernel) by Linus Torvalds, who holds and maintains the copyright to Linux. With the assistance of thousands of developers around the world, it has turned into a robust, stable, and secure operating system, not unlike its other UNIX-based counterparts. Other than the kernel, it is mainly composed of developer-contributed software.

Loopback Address

The loopback address reserved system IP address that is used for diagnostic purposes on a local system. This address is a reserved address and is never used to connect to the network. Any TCP/IP-enabled system with a network adapter will have a loopback address.

Netmask

A 32-bit address similar to the IP address that denotes the most local part of the network; it is a way of denoting which network a given machine belongs to. A machine that does not have the same netmask as other systems on a LAN is not considered as a part of that network.

Nessus

It is a powerful, highly configurable, comprehensive open source security vulnerability assessment tool. It works on most flavours of UNIX and is designed to find security holes on both remote systems and the local system running it.

Plone

Plone is an extension of Zope and provides a CMS (content management system) that takes advantage of the objects provided and managed by Zope. It is through Plone that a CMS portal system is created.

Postfix

Postfix is another UNIX-based mail server application. It is a commonly used alternative to Sendmail and offers more security and is easier to configure.

RPM (Red Hat Package Manager)

RPM can refer to items: either the Linux Rpm program which manages the installation of Red Hat specific software packages or a software packaging format commonly used on Red Hat-based systems.

Router

An internetworking device designed to take network packets from one network and route it on its way to the destination network. A router may perform various actions on the network packets and can pass it forward, drop it, block it, or query another router for the next best path. Modern routers tend to come in the form of a pre-built appliance especially designed for the task at hand; however, PC's can also be used for this task.

Sandbox

A computer-security Sandbox can be either running an application on an untrusted system where the sandbox provides a set of tightly controlled system resources for an application to run. This is often done by virtualizing a system's set of resources such that an application thinks it has real access to the resources but instead is only using a virtual copy. In our particular case for this report, we refer to a Sandbox as a tightly controlled network access where systems from the outside world (i.e. Internet) are able to gain a very tightly controlled network access to a given system.

SELinux (Security Enhanced Linux)

SELinux is a set of modifications/improvements to the Linux kernel made public by the National Security Agency that can implement Mandatory Access Control on a system.

Sendmail

Sendmail is the quite possibly the world's most common mail server application that is utilized on the majority of the world mail server. Originally developed for UNIX-based it has been successfully ported to many other platforms. It is a highly flexible, configurable, and robust.

SMB (Server Message Block)

SMB is a Windows-specific communication protocol that is used to share information and data such as files and network printing. It was developed as a Microsoft-compatible protocol for communicating with non-Windows systems. It is not a TCP/IP protocol but can run on top of it. It is not a service but rather a means for providing a service.

SSL (Secure Sockets Layer)

The Secure Sockets Layer is a TCP/IP protocol developed by Netscape Inc. and RSA Data Security Inc. for use in transmitting information securely over a public network. It uses key-based encryption to ensure that the network is secure and prevent unauthorized systems from listening in on the network stream. It is a low-level protocol; lower than the standard Web-based protocols and is commonly found in e-commerce sites where personal information is exchanged. It is defined in multiple RFC's.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The Transmission Control Protocol/Internet Protocol is a suit of protocols developed by DARPA (Defense Advanced Research Project Agency (U.S. Gov.)) to facilitate and enable communications between different hosts and different networks. Internet Protocol (IP) is a connectionless protocol and makes no guarantees about the reliability of the transmission of data. It is the modern standard for networking and is the foundation for the Internet.

UNIX

A multi-user, multi-tasking, multi-threaded operating system based on a kernel that provides a consistent interface to the user for both interactive and background job processing. UNIX is multi-platform and hardware independent, and supports advanced API's. It is generally considered by the computing industry as the hallmark of scalable, robust, secure, and reliable computing. It was originally developed at AT&T Labs by Dennis Ritchie and Ken Thompson.

Virtual Host

This is a technique specific to Web servers. Through this technique, it is possible to use multiple domain names on one specific Web server. It is also possible to hide the identity of folder(s) via this technology.

WebDAV (Web-based Distributed Authoring and Versioning)

WebDAV is an official extension of the HTTP protocol that aims to make the HTTP protocol both readable and writeable. This means that using the WebDAV protocol it becomes possible to modify, delete, change, or create documents on remote systems.

WMF (Windows Metafile)

WMF is a proprietary Microsoft data format that can be used to store both vector and bitmap-based data.

X Windows

X Windows is a popular graphical windowing system commonly available on UNIX-based platforms. There are also several Windows-based ports. It features a server and a client. The X Windows server portion serves the graphical display to either the local system (connected to the system by the graphics console). The X Windows client accepts X-based connections that can occur either locally or from remote connections. X Windows is very plain by itself and requires a windowing manager to provide advanced graphical features and interfaces. X Windows is a TCP/IP-based protocol.

ZMI (Zope Management Interface)

The ZMI is accessible to authenticated users. It presents a Web-based interface that allows the administrator to view, manage, and control the variously stored objects with the Zope database. Zope objects are stored in an object database, and the ZMI provides a multi-framed view from within a Web browser to better enable the administrator to manage the Zope system.

Zope (Z Object Publishing Environment)

Zope is an open source project that has been written in Python. Zope is a Web server that can publish objects stored in its object database. Natively, Zope supports simple objects such as documents, page templates, and images. To expand its capabilities, third party tools can be used.

This page intentionally left blank.

Distribution list

Document No.: DRDC Valcartier TN 2006-585

LIST PART 1: Internal Distribution by Centre:

- 3 Document Library
- 1 Richard Carbone (author)
- 1 Robert Charpentier
- 1 Yves van Chestein
- 1 Alain Auger
- 1 Michel Lizotte

8 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

DRDC Corporate HQ

- 1 Donna Wood
- 1 Directorate R & D – Knowledge and Information Management (PDF)
- 1 Jack Pagotto
- 1 Eve-Marie Beaudoin

NDHQ (101 Colonel By, Ottawa, K1A 0K2)

- 1 VCDS – CF lessons learned
Attn: LCol Chris Blodgett
- 1 COS IM (DISB project)
Attn: Maj Dave Goldsmith
- 1 COS IM (DISB project)
Attn: Maj Dave Perry
- 1 COS IM (DISB project)
Attn: Ellen De Casmaker
- 1 DJFC
Attn: LCol Rick Johnston
- 1 JIIFC
Attn: LCol Conrad Namiesniowski
- 1 JIIFC
Attn: Maj Art Henry
- 1 JIIFC
Attn: Paul Raven
- 1 IC2S
Lorna Palmer
- 1 CEFCOM J6

	Col Greg Loos
1	Canada COM J6
	LCol Sean Sullivan
	<hr/>
15	TOTAL LIST PART 2
<u>23</u>	<u>TOTAL COPIES REQUIRED</u>

DOCUMENT CONTROL DATA		
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		
1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) DRDC Valcartier	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) Unclassified	
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C, R or U) in parentheses after the title.) (U) Deploying Zope and Plone portals: A low cost solution		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Carbone, R.		
5. DATE OF PUBLICATION (Month and year of publication of document.) October 2006	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 170	6b. NO. OF REFS (Total cited in document.) 13
7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Technical Note		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Knowledge Management Systems Group		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.) 11hg, 11he, 15aw	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)	
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC Valcartier TN 2006-585	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)	
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) <input checked="" type="checkbox"/> Unlimited distribution <input type="checkbox"/> Defence departments and defence contractors; further distribution only as approved <input type="checkbox"/> Defence departments and Canadian defence contractors; further distribution only as approved <input type="checkbox"/> Government departments and agencies; further distribution only as approved <input type="checkbox"/> Defence departments; further distribution only as approved <input type="checkbox"/> Other (please specify):		
12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.)		
13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include		

here abstracts in both official languages unless the text is bilingual.)

(U) In Summer 2005 a task was undertaken to build and implement a rapid portal deployment environment based on a content management system. DRDC projects such as MSOC and ARMADA have seen and reaped the benefit of utilizing portal-based environments. The objective was to implement such a portal based on readily available open source products in order to reduce the costs and yet benefit from a highly configurable, flexible, robust, and low-cost solution. The current portal described in this document is supporting both internal DRDC clients as well as international clients via the TTCP. The main objective of this document is to share the experiences of implementing just such a portal and describe how to build and rapidly deploy one. It also presents how to ensure due diligence with respect to its security.

14. **KEYWORDS, DESCRIPTORS or IDENTIFIERS** (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Linux, open source, Zope, Plone, Apache, virtual host, SSL, certificate, portal, Nessus, security scan, audit, vulnerability scan, sandbox, Postfix, mail redirection

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale



WWW.drdc-rddc.gc.ca

