Title : Remediation Report

Scan Summary	
Scan Name	WebNMS1
Start Time	Tue Feb 21 12:54:49 IST 2006
End Time	Tue Feb 21 12:59:25 IST 2006
Time taken for Scan	4 minutes: 36 seconds
No of Systems	1
Credential Used	Linux credential - Account1
Initiator	admin from gnanasekar.india.adventnet.com
Target Hosts	ms-linuxes1.india.adventnet.com [192.168.117.171]
Vulnerability Group	Complete Scan

Vulnerability Summary	
Total Information Gathered	128 (Vulnerabilities + Missing Patches + Missing SPs + Open Ports)
Missing Patches	104
Missing Service Packs	0
Open Ports	9
Total No fo Vulnerability Found	15
High Risk Vulnerabilities	7
Medium Risk Vulnerabilities	7
Low Rlisk Vulnerabilities	1
Marked as False Positive Vulnerabilities	0
Most Vulnerable Host	ms-linuxes1.india.adventnet.com (7 | 7 | 1)
Most Vulnerable Service	MySQL

Detailed Report - Based on Vulnerabilities [False Positive Not Included]

High **rpc.statd buffer overflow** **RPC**

CVEID : CVE-1999-0018 **Type :** Gain Admin Access

Bugtrack ID :

Threat :

Buffer overflow in statd allows root privileges. There are numerous flaws in RPC which are being actively exploited. Many RPC services execute with elevated privileges that can provide an attacker unauthorized remote root access to vulnerable systems

Solution :

Disable this service or apply patch

Reference :

http://www.sans.org/top20/#u2

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	111	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **rpc.statd file delete vulnerability** **RPC**

CVEID :CVE-1999-0019 **Type :** Integrity

Bugtrack ID :

Threat :

Delete or create a file via rpc.statd, due to invalid information. There are numerous flaws in RPC which are being actively exploited. Many RPC services execute with elevated privileges that can provide an attacker unauthorized remote root access to vulnerable systems

Solution :

Disable this service or apply patch

Reference :

http://www.sans.org/top20/#u2

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	111	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **rpc.statd service** **RPC**

CVEID :CVE-1999-0493 **Type :** Security Protection

Bugtrack ID :

Threat :

rpc.statd allows remote attackers to forward RPC calls to the local operating system via the SM_MON and SM_NOTIFY commands, which in turn could be used to remotely exploit other bugs such as in automountd.

Solution :

Disable this service or apply patch

Reference :

http://www.sans.org/top20/#u2
http://www.cert.org/advisories/CA-1999-05.html

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	111	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **MySQL Remote FULLTEXT Search Denial Of Service Vulnerability** **MySQL**

CVEID :CAN-2004-0956 **Type :** Denial of Service

Bugtrack ID :11432

Threat :

A denial of service vulnerability is present in MySQL in its FULLTEXT search functionality. This is due to failure to handle exceptional search input. The DoS occurs when a MATCH AGAINST query is issued with an opening double quote but no closing double quote.

Solution :

Upgrade to MySQL 4.0.21 or higher

Reference :

http://bugs.mysql.com/bug.php?id=3870
http://dev.mysql.com/downloads/mysql/4.0.html

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **MySQL CREATE FUNCTION arbitrary code execution** **MySQL**

CVEID :CAN-2005-0709 **Type :** Security Protection

Bugtrack ID :

Threat :

MySQL is an open source relational database. It is reported that arbitrary code can be executed on the MySQL database by remote authenticated users if they have INSERT and DELETE privileges. This vulnerability is due to insufficient input validation which may be leveraged to load and execute a malicious library in the context of the MySQL process. The issue is reported to exist in MySQL versions prior to 4.0.24 and 4.1.10a

Solution :

The vulnerability is fixed in MySQL 4.0.24 and 4.1.10a which are available for download in MySQL website.

Reference :

http://marc.theaimsgroup.com/?l=bugtraq&m=111066115808506&w=2
http://www.mysql.com/

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **Mysql CREATE FUNCTION mysql.func table arbitrary library injection** **MySQL**

CVEID :CAN-2005-0710 **Type :** Security Protection

Bugtrack ID :12781

Threat :

MySQL is a multi-user, multi-threaded relational database management system. It has been reported that versions 4.0.23 and earlier, and 4.1.x up to 4.1.10, allows remote users with INSERT and DELETE privileges to bypass library path restrictions and execute arbitrary libraries by using INSERT INTO to modify the mysql.func table, which is processed by the udf_init function.

Solution :

Upgrade to 4.0.24 or 4.1.10a or most recent version of MySql. For more information, please look at the vendor site : http://www.mysql.com/

Reference :

http://www.mysql.com/

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

High **Weak user account detected** **Telnet**

CVEID :CVE-1999-0502 **Type :** Weak User Accounts and Passwords

Bugtrack ID :

Threat :

A weak user account is detected in the remote system. Please use a strong password. The user name and password are shown below.

Solution :

Please use a strong password

Reference :

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	23	Red Hat Enterprise Linux ES 4

RESULT :
UserName: guest Password: guest

Medium **OpenSSH 3.9 and earlier stored passwords in plain text file** **SSH**

CVEID :CAN-2005-2666 **Type :** Security Protection

Bugtrack ID :

Threat :

OpenSSH is a secure remote access / command execution protocol. It has been reported that versions 3.9p1 and earlier stores the passwords, hostnames, ip in a plain text file. This makes it easier for an attacker that has compromised an SSH user's account to generate a list of additional targets that are more likely to have the same password or key.

Solution :

This vulnerabiltiy is fixed in OpenSSH 4.0. Upgrade to 4.0 or most recent version of OpenSSH. The latest version of OpenSSH can be downloaded from http://www.openssh.com/portable.html#http

Reference :

http://nms.csail.mit.edu/projects/ssh/
http://www.openssh.com/

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	22	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

Medium **OpenSSH GSSAPI Credential Disclosure Vulnerability** **SSH**

CVEID :CAN-2005-2798 **Type :** Security Protection

Bugtrack ID :14729

Threat :

OpenSSH is a secure remote access / command execution protocol. It has been reported that versions 4.1 and earlier are prone to GSSAPI Credential Disclosure Vulnerability. sshd in OpenSSH, when GSSAPIDelegateCredentials is enabled, allows GSSAPI credentials to be delegated to clients who log in using non -GSSAPI methods, which could cause those credentials to be exposed to untrusted users or hosts. This may lead to further attacks over the vulnerable system.

Solution :

This issue is addressed in version 4.2. Upgrade to 4.2 or most recent version of OpenSSH. The latest version of OpenSSH can be downloaded from : http://www.openssh.com/

Reference :

http://www.mindrot.org/pipermail/openssh-unix-announce/2005-September/000083.html
http://www.openssh.com/

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	22	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

Medium **MySQL Database Unauthorized GRANT Privilege Vulnerability** **MySQL**

CVEID :CAN-2004-0957 **Type :** Security Protection

Bugtrack ID :11435

Threat :

The remote host is running a verison of MySQL which is older than 4.0.21. Those versions of MySQL are reported susceptible to an unauthorized database GRANT privilege vulnerability. This issue is due to a failure of the application to ensure that users have sufficient privileges to issue the GRANT command.

By exploiting this vulnerability, attackers may be able to gain unauthorized access to databases. This may allow them to read or modify the contents of potentially sensitive databases located on the same database server.

Solution :

Upgrade to MySQL 4.0.21 or higher

Reference :

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

Medium **MySQL Multiple Local Vulnerabilities** **MySQL**

CVEID :CAN-2004-0837 **Type :** Denial of Service

Bugtrack ID :11357

Threat :

The remote host is running a version of MySQL which is older than 4.0.21 or 3.23.59. Vulnerabilities in those versions may allow an attacker to bypass security restrictions or cause a denial of service condition. These issues are due to errors in ALTER TABLE implementation.

Solution :

Upgrade to MySQL 3.23.59 or 4.0.21 or latest

Reference :

http://bugs.mysql.com/bug.php?id=3270
http://bugs.mysql.com/bug.php?id=2408

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

Medium **Stack-based buffer overflow in Mysql 4.0-4.0.24, 4.1-4.1.12, and 5.0-5.0.6** **MySQL**

CVEID :CAN-2005-2558 **Type :** Denial of Service

Bugtrack ID :14509

Threat :

The remote host is running a vulnerable version of MySQL. It has been reported that versions 4.0 throuh 4.0.24, 4.1 through 4.1.12 and 5.0 through 5.0.6 are prone to stack based buffer overflow vulnerability. It is possible for any remote authenticated users who can create user-defined functions to execute arbitrary code via a long function_name field. The issue is present in the init_syms function.

Solution :

MySQL addressed this issue in the versions 4.0.25, 4.1.13 and 5.0.7. Upgrade to 4.0.25, or 4.1.13 or 5.0.7 or most recent version of MySQL. The latest version of mysql can be downloaded from : http://www.mysql.com/

Reference :

http://www.mysql.com/
http://marc.theaimsgroup.com/?l=bugtraq&m=112354450412427&w=2

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	3306	Red Hat Enterprise Linux ES 4

RESULT :
No Results Available

Medium **Anonymous FTP login enabled** **FTP**

CVEID :CAN-1999-0497 **Type :** Confidentiality

Bugtrack ID :

Threat :

The FTP server allows anonymous logins. Anyone can access the server with user name as "anonymous" and with any password. The FTP server may contain sensitive files using which attackers can gain valuable information. The contents of the FTP root are listed below.

Solution :

If you do not want to share the data with anyone, disable this account. Use a password-protected account if you want to share files.

Reference :

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	21	Red Hat Enterprise Linux ES 4

RESULT :
drwxr-xr-x 2 0 0 4096 Jun 28 2005 pub

Medium **Telnet service is running** **Telnet**

CVEID :CAN-1999-0619 **Type :** OpenPorts

Bugtrack ID :

Threat :

The Telnet service is running in the remote host. The data between telnet client and server are transmitted in clear text and are not encrypted and hence data can be easily sniffed. This includes logins and passwords.

Solution :

Use SSH for secure communication

Reference :

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	23	Red Hat Enterprise Linux ES 4
RESULT : No Results Available			

Low **Apache Remote Username Enumeration Vulnerability** **HTTP**

CVEID :CAN-2001-1013 **Type :** Misconfigurations

Bugtrack ID :3335

Threat :

Apache web server, when installed with a default misconfiguration, could allow remote attackers to determine whether a give username exists on the system. URL: http://www.example.com/~<username>

In a case where <username> is a valid user account, and has been configured with a homepage, the server responds with the user"s homepage.

When <username> exists on the system, but has not been assigned a homepage document, the server returns the message "You don"t have permission to access /~username on this server."

However, if the tested username does not exist as an account on the system, the Apache server"s response includes the message "The requested URL /~username was not found on this server."

Becaue of the difference in the error message, an attacker can find out a valid account name and can do further attacks.

Solution :

Add the following line to httpd.conf
UserDir Disabled

Reference :

Result :

IP Address	Host Name	Port	Operating Systems
192.168.117.171	ms-linuxes1.india.adventnet.com	9090	Red Hat Enterprise Linux ES 4
RESULT : http://192.168.117.171:9090/~root			

Service Pack Details - Based on Hosts

Missing Patches - Based on Hosts

192.168.117.171 **ms-linuxes1.india.adventnet.com** Red Hat Enterprise Linux ES 4

Unrated **Moderate: openldap and nss_ldap security update**

BULLETINID :

RHSA-2005:767-01

Description :

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools.

The nss_ldap module is an extension for use with GNU libc which allows applications to, without internal modification, consult a directory service using LDAP to supplement information that would be read from local files such as /etc/passwd, /etc/group, and /etc/shadow.

A bug was found in the way OpenLDAP, nss_ldap, and pam_ldap refer LDAP servers. If a client connection is referred to a different server, it is possible that the referred connection will not be encrypted even if the client has 'ssl start_tls' in its ldap.conf file. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2069 to this issue.

A bug was found in the way the pam_ldap module processed certain failure messages. If the server includes supplemental data in an authentication failure result message, but the data does not include any specific error code, the pam_ldap module would proceed as if the authentication request had succeeded, and authentication would succeed. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2641 to this issue.

Additionally the following issues are corrected in this erratum.

- - The OpenLDAP upgrading documentation has been updated.

- - Fix a database deadlock locking issue.

- - A fix where slaptest segfaults on exit after successful check.

- - The library libslapd_db-4.2.so is now located in an architecture-dependent directory.

- - The LDAP client no longer enters an infinite loop when the server returns a reference to itself.

- - The pam_ldap module adds the ability to check user passwords using a directory server to PAM-aware applications.

- - The directory server can now include supplemental information regarding the state of the user's account if a client indicates that it supports such a feature.

All users of OpenLDAP and nss_ldap are advised to upgrade to these updated packages, which contain backported fixes that resolve these issues.

Patches To Apply :

compat-openldap-2.1.30-4.i386.rpm

nss_ldap-226-10.i386.rpm

openldap-2.2.13-4.i386.rpm

openldap-clients-2.2.13-4.i386.rpm

openldap-devel-2.2.13-4.i386.rpm

openldap-servers-2.2.13-4.i386.rpm

openldap-servers-sql-2.2.13-4.i386.rpm

Unrated **Moderate: curl security update**

BULLETINID :

RHSA-2005:807-00

Description :

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols.

A stack based buffer overflow bug was found in cURL's NTLM authentication module. It is possible to execute arbitrary code on a user's machine if the user can be tricked into connecting to a malicious web server using NTLM authentication. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-3185 to this issue.

All users of curl are advised to upgrade to these updated packages, which contain a backported patch that resolve this issue.

Patches To Apply :

curl-7.12.1-6.rhel4.i386.rpm

curl-devel-7.12.1-6.rhel4.i386.rpm

Unrated **Moderate: ethereal security update**

BULLETINID :

RHSA-2005:809-01

Description :

The ethereal package is a program for monitoring network traffic.

A number of security flaws have been discovered in Ethereal. On a system where Ethereal is running, a remote attacker could send malicious packets to trigger these flaws and cause Ethereal to crash or potentially execute arbitrary code. The Common Vulnerabilities and Exposures project has assigned the names CVE-2005-3241, CVE-2005-3242, CVE-2005-3243, CVE-2005-3244, CVE-2005-3245, CVE-2005-3246, CVE-2005-3247, CVE-2005-3248, CVE-2005-3249, and CVE-2005-3184 to these issues.

Users of ethereal should upgrade to these updated packages, which contain version 0.10.13 and are not vulnerable to these issues.

Patches To Apply :

ethereal-0.10.13-1.EL4.1.i386.rpm

ethereal-gnome-0.10.13-1.EL4.1.i386.rpm

Unrated	**Critical: firefox security update**

BULLETINID :

RHSA-2005:176-01

Description :

Mozilla Firefox is an open source Web browser.

A bug was found in the Firefox 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 CAN-2005-0255 to this issue.

A bug was found in the way Firefox handles pop-up windows. It is possible for a malicious website to control the content in an unrelated site's pop-up window. (CAN-2004-1156)

A bug was found in the way Firefox allows plug-ins to load privileged content into a frame. It is possible that a malicious webpage could trick a user into clicking in certain places to modify configuration settings or execute arbitrary code. (CAN-2005-0232 and CAN-2005-0527).

A flaw was found in the way Firefox displays international domain names. It is possible for an attacker to display a valid URL, tricking the user into thinking they are viewing a legitimate webpage when they are not. (CAN-2005-0233)

A bug was found in the way Firefox handles plug-in temporary files. A malicious local user could create a symlink to a victims directory, causing it to be deleted when the victim exits Firefox. (CAN-2005-0578)

A bug has been found in one of Firefox's UTF-8 converters. It may be possible for an attacker to supply a specially crafted UTF-8 string to the buggy converter, leading to arbitrary code execution. (CAN-2005-0592)

A bug was found in the Firefox javascript security manager. If a user drags a malicious link to a tab, the javascript security manager is bypassed which could result in remote code execution or information disclosure. (CAN-2005-0231)

A bug was found in the way Firefox displays the HTTP authentication prompt. When a user is prompted for authentication, the dialog window is displayed over the active tab, regardless of the tab that caused the pop-up to appear and could trick a user into entering their username and password for a trusted site. (CAN-2005-0584)

A bug was found in the way Firefox displays the save file dialog. It is possible for a malicious webserver to spoof the Content-Disposition header, tricking the user into thinking they are downloading a different filetype. (CAN-2005-0586)

A bug was found in the way Firefox handles users 'down-arrow' through auto completed choices. When an autocomplete choice is selected, the information is copied into the input control, possibly allowing a malicious web site to steal information by tricking a user into arrowing through autocompletion choices. (CAN-2005-0589)

Several bugs were found in the way Firefox displays the secure site icon. It is possible that a malicious website could display the secure site icon along with incorrect certificate information. (CAN-2005-0593)

A bug was found in the way Firefox displays the download dialog window. A malicious site can obfuscate the content displayed in the source field, tricking a user into thinking they are downloading content from a trusted

source. (CAN-2005-0585)

A bug was found in the way Firefox handles xsl:include and xsl:import directives. It is possible for a malicious website to import XSLT stylesheets from a domain behind a firewall, leaking information to an attacker. (CAN-2005-0588)

A bug was found in the way Firefox displays the installation confirmation dialog. An attacker could add a long user:pass before the true hostname, tricking a user into thinking they were installing content from a trusted source. (CAN-2005-0590)

A bug was found in the way Firefox displays download and security dialogs. An attacker could cover up part of a dialog window tricking the user into clicking 'Allow' or 'Open', which could potentially lead to arbitrary code execution. (CAN-2005-0591)

Users of Firefox are advised to upgrade to this updated package which contains Firefox version 1.0.1 and is not vulnerable to these issues.

Patches To Apply :

firefox-1.0.1-1.4.3.i386.rpm

Unrated **Critical: firefox security update**

BULLETINID :

RHSA-2005:768-01

Description :

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 CAN-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.

Patches To Apply :

firefox-1.0.6-1.4.2.i386.rpm

Unrated **Important: gaim security update**

BULLETINID :

RHSA-2005:215-01

Description :

The Gaim application is a multi-protocol instant messaging client.

Two HTML parsing bugs were discovered in Gaim. It is possible that a remote attacker could send a specially crafted message to a Gaim client, causing it to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-0208 and CAN-2005-0473 to these issues.

A bug in the way Gaim processes SNAC packets was discovered. It is possible that a remote attacker could send a specially crafted SNAC packet to a Gaim client, causing the client to stop responding. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0472 to this issue.

Additionally, various client crashes, memory leaks, and protocol issues have been resolved.

Users of Gaim are advised to upgrade to this updated package which contains Gaim version 1.1.4 and is not vulnerable to these issues.

Patches To Apply :

gaim-1.1.4-1.EL4.i386.rpm

Unrated	**Important: gaim security update**

BULLETINID :

RHSA-2005:365-01

Description :

The Gaim application is a multi-protocol instant messaging client.

A buffer overflow bug was found in the way gaim escapes HTML. It is possible that a remote attacker could send a specially crafted message to a Gaim client, causing it to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0965 to this issue.

A bug was found in several of gaim's IRC processing functions. These functions fail to properly remove various markup tags within an IRC message. It is possible that a remote attacker could send a specially crafted message to a Gaim client connected to an IRC server, causing it to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0966 to this issue.

A bug was found in gaim's Jabber message parser. It is possible for a remote Jabber user to send a specially crafted message to a Gaim client, causing it to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0967 to this issue.

In addition to these denial of service issues, multiple minor upstream bugfixes are included in this update.

Users of Gaim are advised to upgrade to this updated package which contains Gaim version 1.2.1 and is not vulnerable to these issues.

Patches To Apply :

gaim-1.2.1-4.el4.i386.rpm

Unrated	**Critical: gaim security update**

BULLETINID :

RHSA-2005:429-01

Description :

The Gaim application is a multi-protocol instant messaging client.

A stack based buffer overflow bug was found in the way gaim processes a message containing a URL. A remote attacker could send a carefully crafted message resulting in the execution of arbitrary code on a victim's machine. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1261 to this issue.

A bug was found in the way gaim handles malformed MSN messages. A remote attacker could send a carefully crafted MSN message causing gaim to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1262 to this issue.

Users of Gaim are advised to upgrade to this updated package which contains backported patches and is not vulnerable to these issues.

Patches To Apply :

gaim-1.2.1-6.el4.i386.rpm

Unrated **Important: gdk-pixbuf security update**

BULLETINID :

RHSA-2005:810-01

Description :

The gdk-pixbuf package contains an image loading library used with the GNOME GUI desktop environment.

A bug was found in the way gdk-pixbuf processes XPM images. An attacker could create a carefully crafted XPM file in such a way that it could cause an application linked with gdk-pixbuf to execute arbitrary code when the file was opened by a victim. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-3186 to this issue.

Ludwig Nussel discovered an integer overflow bug in the way gdk-pixbuf processes XPM images. An attacker could create a carefully crafted XPM file in such a way that it could cause an application linked with gdk-pixbuf to execute arbitrary code or crash when the file was opened by a victim. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2976 to this issue.

Ludwig Nussel also discovered an infinite-loop denial of service bug in the way gdk-pixbuf processes XPM images. An attacker could create a carefully crafted XPM file in such a way that it could cause an application linked with gdk-pixbuf to stop responding when the file was opened by a victim. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2975 to this issue.

Users of gdk-pixbuf are advised to upgrade to these updated packages, which contain backported patches and are not vulnerable to these issues.

Patches To Apply :

gdk-pixbuf-0.22.0-17.el4.3.i386.rpm

gdk-pixbuf-devel-0.22.0-17.el4.3.i386.rpm

Unrated	**Critical: HelixPlayer security update**

BULLETINID :

RHSA-2005:271-01

Description :

HelixPlayer is a media player.

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 CAN-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 CAN-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.

Patches To Apply :

HelixPlayer-1.0.3-1.i386.rpm

Unrated **Critical: HelixPlayer security update**

BULLETINID :

RHSA-2005:392-03

Description :

HelixPlayer is a media player.

A buffer overflow bug was found in the way HelixPlayer processes RAM files. An attacker could create a specially crafted RAM file which could execute arbitrary code when opened by a user. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0755 to this issue.

All users of HelixPlayer are advised to upgrade to this updated package, which contains HelixPlayer version 10.0.4 and is not vulnerable to this issue.

Patches To Apply :

HelixPlayer-1.0.4-1.1.EL4.2.i386.rpm

Unrated **Important: kernel security update**

BULLETINID :

RHSA-2005:808-01

Description :

The Linux kernel handles the basic functions of the operating system.

An issue was discovered that affects how page attributes are changed by the kernel. Video drivers, which sometimes map kernel pages with a different caching policy than write-back, are now expected to function correctly. This change affects the x86, AMD64, and Intel EM64T architectures.

In addition the following security bugs were fixed:

The set_mempolicy system call did not check for negative numbers in the policy field. An unprivileged local user could use this flaw to cause a denial of service (system panic). (CVE-2005-3053)

A flaw in ioremap handling on AMD 64 and Intel EM64T systems. An unprivileged local user could use this flaw to cause a denial of service or minor information leak. (CVE-2005-3108)

A race condition in the ebtables netfilter module. On a SMP system that is operating under a heavy load this flaw may allow remote attackers to cause a denial of service (crash). (CVE-2005-3110)

A memory leak was found in key handling. An unprivileged local user could use this flaw to cause a denial of service. (CVE-2005-3119)

A flaw in the Orinoco wireless driver. On systems running the vulnerable drive, a remote attacker could send carefully crafted packets which would divulge the contents of uninitialized kernel memory. (CVE-2005-3180)

A memory leak was found in the audit system. An unprivileged local user could use this flaw to cause a denial of service. (CVE-2005-3181)

All Red Hat Enterprise Linux 4 users are advised to upgrade their kernels to the packages associated with their machine architectures and configurations as listed in this erratum.

Patches To Apply :

kernel-2.6.9-22.0.1.EL.i686.rpm

kernel-devel-2.6.9-22.0.1.EL.i686.rpm

kernel-doc-2.6.9-22.0.1.EL.noarch.rpm

kernel-hugemem-devel-2.6.9-22.0.1.EL.i686.rpm

kernel-smp-devel-2.6.9-22.0.1.EL.i686.rpm

Unrated **Important: libungif security update**

BULLETINID :

RHSA-2005:828-01

Description :

The libungif package contains a shared library of functions for loading and saving GIF format image files.

Several bugs in the way libungif decodes GIF images were discovered. An attacker could create a carefully crafted GIF image file in such a way that it could cause an application linked with libungif to crash or execute arbitrary code when the file is opened by a victim. The Common Vulnerabilities and Exposures project has assigned the names CVE-2005-2974 and CVE-2005-3350 to these issues.

All users of libungif are advised to upgrade to these updated packages, which contain backported patches that resolve these issues.

Patches To Apply :

libungif-4.1.3-1.el4.2.i386.rpm

libungif-devel-4.1.3-1.el4.2.i386.rpm

libungif-progs-4.1.3-1.el4.2.i386.rpm

Unrated **Low: lm_sensors security update**

BULLETINID :

RHSA-2005:825-01

Description :

The lm_sensors package includes a collection of modules for general SMBus access and hardware monitoring. This package requires special support which is not in standard version 2.2 kernels.

A bug was found in the way the pwmconfig tool creates temporary files. It is possible that a local attacker could leverage this flaw to overwrite arbitrary files located on the system. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2672 to this issue.

Users of lm_sensors are advised to upgrade to these updated packages, which contain a backported patch that resolves this issue.

Patches To Apply :

lm_sensors-2.8.7-2.40.3.i386.rpm

lm_sensors-devel-2.8.7-2.40.3.i386.rpm

Unrated **Critical: lynx security update**

BULLETINID :

RHSA-2005:803-01

Description :

Lynx is a text-based Web browser.

Ulf Harnhammar discovered a stack overflow bug in Lynx when handling connections to NNTP (news) servers. An attacker could create a web page redirecting to a malicious news server which could execute arbitrary code as the user running lynx. The Common Vulnerabilities and Exposures project assigned the name CAN-2005-3120 to this issue.

Users should update to this erratum package, which contains a backported patch to correct this issue.

Patches To Apply :

lynx-2.8.5-18.1.i386.rpm

Unrated **Critical: lynx security update**

BULLETINID :

RHSA-2005:839-01

Description :

Lynx is a text-based Web browser.

An arbitrary command execute bug was found in the lynx 'lynxcgi:' URI handler. An attacker could create a web page redirecting to a malicious URL which could execute arbitrary code as the user running lynx. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-2929 to this issue.

Users should update to this erratum package, which contains a backported patch to correct this issue.

Patches To Apply :

lynx-2.8.5-18.2.i386.rpm

Unrated **Critical: mozilla security update**

BULLETINID :

RHSA-2005:277-01

Description :

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor.

A bug was found in the Mozilla 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 CAN-2005-0255 to this issue.

Please note that other security issues have been found that affect Mozilla. These other issues have a lower severity, and are therefore planned to be released as additional security updates in the future.

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

Patches To Apply :

mozilla-1.7.3-19.EL4.i386.rpm

mozilla-chat-1.7.3-19.EL4.i386.rpm

mozilla-devel-1.7.3-19.EL4.i386.rpm

mozilla-dom-inspector-1.7.3-19.EL4.i386.rpm

mozilla-js-debugger-1.7.3-19.EL4.i386.rpm

mozilla-mail-1.7.3-19.EL4.i386.rpm

mozilla-nspr-1.7.3-19.EL4.i386.rpm

mozilla-nspr-devel-1.7.3-19.EL4.i386.rpm

mozilla-nss-1.7.3-19.EL4.i386.rpm

mozilla-nss-devel-1.7.3-19.EL4.i386.rpm

Unrated	**Important: Mozilla security update**

BULLETINID :

RHSA-2005:386-01

Description :

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor.

Vladimir V. Perepelitsa discovered a bug in the way Mozilla handles anonymous functions during regular expression string replacement. It is possible for a malicious web page to capture a random block of browser memory. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0989 to this issue.

Doron Rosenberg discovered a bug in the way Mozilla displays pop-up windows. If a user choses to open a pop-up window whose URL is malicious javascript, the script will be executed with elevated privileges. (CAN-2005-1153)

A bug was found in the way Mozilla handles the javascript global scope for a window. It is possible for a malicious web page to define a global variable known to be used by a different site, allowing malicious code to be executed in the context of the site. (CAN-2005-1154)

Michael Krax discovered a bug in the way Mozilla handles favicon links. A malicious web page can programatically define a favicon link tag as javascript, executing arbitrary javascript with elevated privileges. (CAN-2005-1155)

Michael Krax discovered a bug in the way Mozilla installed search plugins. If a user chooses to install a search plugin from a malicious site, the new plugin could silently overwrite an existing plugin. This could allow the malicious plugin to execute arbitrary code and stealm sensitive information. (CAN-2005-1156 CAN-2005-1157)

A bug was found in the way Mozilla validated several XPInstall related javascript objects. A malicious web page could pass other objects to the XPInstall objects, resulting in the javascript interpreter jumping to arbitrary locations in memory. (CAN-2005-1159)

A bug was found in the way the Mozilla privileged UI code handled DOM nodes from the content window. A malicious web page could install malicious javascript code or steal data requiring a user to do commonplace actions such as clicking a link or opening the context menu. (CAN-2005-1160)

Users of Mozilla are advised to upgrade to this updated package which contains Mozilla version 1.7.7 to correct these issues.

Patches To Apply :

mozilla-1.7.7-1.4.2.i386.rpm

mozilla-chat-1.7.7-1.4.2.i386.rpm

mozilla-devel-1.7.7-1.4.2.i386.rpm

mozilla-dom-inspector-1.7.7-1.4.2.i386.rpm

mozilla-js-debugger-1.7.7-1.4.2.i386.rpm

mozilla-mail-1.7.7-1.4.2.i386.rpm

mozilla-nspr-1.7.7-1.4.2.i386.rpm

mozilla-nspr-devel-1.7.7-1.4.2.i386.rpm

mozilla-nss-1.7.7-1.4.2.i386.rpm

mozilla-nss-devel-1.7.7-1.4.2.i386.rpm

Unrated **Critical: mozilla security update**

BULLETINID :

RHSA-2005:769-01

Description :

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 CAN-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.

Patches To Apply :

mozilla-1.7.10-1.4.2.i386.rpm

mozilla-chat-1.7.10-1.4.2.i386.rpm

mozilla-devel-1.7.10-1.4.2.i386.rpm

mozilla-dom-inspector-1.7.10-1.4.2.i386.rpm

mozilla-js-debugger-1.7.10-1.4.2.i386.rpm

mozilla-mail-1.7.10-1.4.2.i386.rpm

mozilla-nspr-1.7.10-1.4.2.i386.rpm

mozilla-nspr-devel-1.7.10-1.4.2.i386.rpm

mozilla-nss-1.7.10-1.4.2.i386.rpm

mozilla-nss-devel-1.7.10-1.4.2.i386.rpm

Unrated **Moderate: netpbm security update**

BULLETINID :

RHSA-2005:793-01

Description :

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.

A bug was found in the way netpbm converts Portable Anymap (PNM) files into Portable Network Graphics (PNG). The usage of uninitialised variables in the pnmtopng code allows an attacker to change stack contents when converting to PNG files with pnmtopng using the '-trans' option. This may allow an attacker to execute arbitrary code. The Common Vulnerabilities and Exposures project assigned the name CAN-2005-2978 to this issue.

All users of netpbm should upgrade to the updated packages, which contain a backported patch to resolve this issue.

Patches To Apply :

netpbm-10.25-2.EL4.2.i386.rpm

netpbm-devel-10.25-2.EL4.2.i386.rpm

netpbm-progs-10.25-2.EL4.2.i386.rpm

Unrated	**Moderate: openssl security update**

BULLETINID :

RHSA-2005:800-01

Description :

OpenSSL is a toolkit that implements Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

OpenSSL contained a software work-around for a bug in SSL handling in Microsoft Internet Explorer version 3.0.2. This work-around is enabled in most servers that use OpenSSL to provide support for SSL and TLS. Yutaka Oiwa discovered that this work-around could allow an attacker, acting as a 'man in the middle' to force an SSL connection to use SSL 2.0 rather than a stronger protocol such as SSL 3.0 or TLS 1.0. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2969 to this issue.

A bug was also fixed in the way OpenSSL creates DSA signatures. A cache timing attack was fixed in RHSA-2005-476 which caused OpenSSL to do private key calculations with a fixed time window. The DSA fix for this was not complete and the calculations are not always performed within a fixed-window. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0109 to this issue.

Users are advised to upgrade to these updated packages, which remove the MISE 3.0.2 work-around and contain patches to correct these issues.

Note: After installing this update, users are advised to either restart all services that use OpenSSL or restart their system.

Patches To Apply :

openssl-0.9.7a-43.4.i386.rpm

openssl-0.9.7a-43.4.i686.rpm

openssl-devel-0.9.7a-43.4.i386.rpm

openssl-perl-0.9.7a-43.4.i386.rpm

openssl096b-0.9.6b-22.4.i386.rpm

Unrated	**Moderate: openssl096b security update**

BULLETINID :

RHSA-2005:830-00

Description :

The OpenSSL toolkit implements Secure Sockets Layer (SSL v2/v3), Transport Layer Security (TLS v1) protocols, and serves as a full-strength general purpose cryptography library. OpenSSL 0.9.6b libraries are provided for Red Hat Enterprise Linux 3 and 4 to allow compatibility with legacy applications.

Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool uncovered a null-pointer assignment in the do_change_cipher_spec() function. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server that uses the OpenSSL library in such a way as to cause OpenSSL to crash. Depending on the server this could lead to a denial of service. (CVE-2004-0079)

This issue was reported as not affecting OpenSSL versions prior to 0.9.6c, and testing with the Codenomicon Test Tool showed that OpenSSL 0.9.6b as shipped as a compatibility library with Red Hat Enterprise Linux 3 and 4 did not crash. However, an alternative reproducer has been written which shows that this issue does affect versions of OpenSSL prior to 0.9.6c.

Note that Red Hat does not ship any applications with Red Hat Enterprise Linux 3 or 4 that use these compatibility libraries.

Users of the OpenSSL096b compatibility package are advised to upgrade to these updated packages, which contain a patch provided by the OpenSSL group that protect against this issue.

Patches To Apply :

openssl096b-0.9.6b-22.42.i386.rpm

Unrated	**Low: pam security update**

BULLETINID :

RHSA-2005:805-01

Description :

PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set an authentication policy without having to recompile programs that handle authentication.

A bug was found in the way PAM's unix_chkpwd helper program validates user passwords when SELinux is enabled. Under normal circumstances, it is not possible for a local non-root user to verify the password of another local user with the unix_chkpwd command. A patch applied that adds SELinux functionality makes it possible for a local user to use brute force password guessing techniques against other local user accounts. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-2977 to this issue.

All users of pam should upgrade to this updated package, which contains backported patches to correct these issues.

Patches To Apply :

pam-0.77-66.13.i386.rpm

pam-devel-0.77-66.13.i386.rpm

Unrated	**Important: perl security update**

BULLETINID :

RHSA-2005:103-01

Description :

Perl is a high-level programming language commonly used for system administration utilities and Web programming.

Kevin Finisterre discovered a stack based buffer overflow flaw in sperl, the Perl setuid wrapper. A local user could create a sperl executable script with a carefully created path name, overflowing the buffer and leading to root privilege escalation. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0156 to this issue.

Kevin Finisterre discovered a flaw in sperl which can cause debugging information to be logged to arbitrary files. By setting an environment variable, a local user could cause sperl to create, as root, files with arbitrary filenames, or append the debugging information to existing files. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0155 to this issue.

An unsafe file permission bug was discovered in the rmtree() function in the File::Path module. The rmtree() function removes files and directories in an insecure manner, which could allow a local user to read or delete arbitrary files. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0452 to this issue.

Users of Perl are advised to upgrade to this updated package, which contains backported patches to correct these issues.

Patches To Apply :

perl-5.8.5-12.1.i386.rpm

perl-suidperl-5.8.5-12.1.1.i386.rpm

Unrated	**Moderate: php security update**

BULLETINID :

RHSA-2005:831-01

Description :

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Web server.

A flaw was found in the way PHP registers global variables during a file upload request. A remote attacker could submit a carefully crafted multipart/form-data POST request that would overwrite the $GLOBALS array, altering expected script behavior, and possibly leading to the execution of arbitrary PHP commands. Please note that this vulnerability only affects installations which have register_globals enabled in the PHP configuration file, which is not a default or recommended option. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-3390 to this issue.

A flaw was found in the PHP parse_str() function. If a PHP script passes only one argument to the parse_str() function, and the script can be forced to abort execution during operation (for example due to the memory_limit setting), the register_globals may be enabled even if it is disabled in the PHP configuration file. This vulnerability only affects installations that have PHP scripts using the parse_str function in this way. (CVE-2005-3389)

A Cross-Site Scripting flaw was found in the phpinfo() function. If a victim can be tricked into following a malicious URL to a site with a page displaying the phpinfo() output, it may be possible to inject javascript or HTML content into the displayed page or steal data such as cookies. This vulnerability only affects installations which allow users to view the output of the phpinfo() function. As the phpinfo() function outputs a large amount of information about the current state of PHP, it should only be used during debugging or if protected by authentication. (CVE-2005-3388)

A denial of service flaw was found in the way PHP processes EXIF image data. It is possible for an attacker to cause PHP to crash by supplying carefully crafted EXIF image data. (CVE-2005-3353)

Users of PHP should upgrade to these updated packages, which contain backported patches that resolve these issues.

Patches To Apply :

php-4.3.9-3.9.i386.rpm

php-devel-4.3.9-3.9.i386.rpm

php-domxml-4.3.9-3.9.i386.rpm

php-gd-4.3.9-3.9.i386.rpm

php-imap-4.3.9-3.9.i386.rpm

php-ldap-4.3.9-3.9.i386.rpm

php-mbstring-4.3.9-3.9.i386.rpm

php-ncurses-4.3.9-3.9.i386.rpm

php-odbc-4.3.9-3.9.i386.rpm

php-pear-4.3.9-3.9.i386.rpm

php-pgsql-4.3.9-3.9.i386.rpm

php-snmp-4.3.9-3.9.i386.rpm

php-xmlrpc-4.3.9-3.9.i386.rpm

Unrated **Important: postgresql security update**

BULLETINID :

RHSA-2005:138-01

Description :

A flaw in the LOAD command in PostgreSQL was discovered. A local user could use this flaw to load arbitrary shared libraries and therefore execute arbitrary code, gaining the privileges of the PostgreSQL server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0227 to this issue.

A permission checking flaw in PostgreSQL was discovered. A local user could bypass the EXECUTE permission check for functions by using the CREATE AGGREGATE command. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0244 to this issue.

Multiple buffer overflows were found in PL/PgSQL. A database user who has permissions to create plpgsql functions could trigger this flaw which could lead to arbitrary code execution, gaining the privileges of the PostgreSQL server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-0245 and CAN-2005-0247 to these issues.

A flaw in the integer aggregator (intagg) contrib module for PostgreSQL was found. A user could create carefully crafted arrays and cause a denial of service (crash). The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0246 to this issue.

The update also fixes some minor problems, notably conflicts with SELinux.

Users of postgresql should update to these erratum packages that contain patches and are not vulnerable to these issues.

Patches To Apply :

postgresql-7.4.7-2.RHEL4.1.i386.rpm

postgresql-contrib-7.4.7-2.RHEL4.1.i386.rpm

postgresql-devel-7.4.7-2.RHEL4.1.i386.rpm

postgresql-docs-7.4.7-2.RHEL4.1.i386.rpm

postgresql-jdbc-7.4.7-2.RHEL4.1.i386.rpm

postgresql-libs-7.4.7-2.RHEL4.1.i386.rpm

postgresql-pl-7.4.7-2.RHEL4.1.i386.rpm

postgresql-python-7.4.7-2.RHEL4.1.i386.rpm

postgresql-server-7.4.7-2.RHEL4.1.i386.rpm

postgresql-tcl-7.4.7-2.RHEL4.1.i386.rpm

postgresql-test-7.4.7-2.RHEL4.1.i386.rpm

Unrated **Moderate: thunderbird security update**

BULLETINID :

RHSA-2005:094-01

Description :

Thunderbird is a standalone mail and newsgroup client.

A bug was found in the way Thunderbird handled cookies when loading content over HTTP regardless of the user's preference. It is possible that a particular user could be tracked through the use of malicious mail messages which load content over HTTP. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0149 to this issue.

Users of Thunderbird are advised to upgrade to this updated package, which contains Thunderbird version 1.0 and is not vulnerable to this issue.

Patches To Apply :

thunderbird-1.0-1.1.EL4.i386.rpm

Unrated **Important: thunderbird security update**

BULLETINID :

RHSA-2005:791-01

Description :

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 mail, which when viewed by the victim would cause Thunderbird to crash or possibly execute arbitrary code. Thunderbird as shipped with Red Hat Enterprise Linux 4 must have international domain names enabled by the user in order to be vulnerable to this issue. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-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 HTML mail containing Unicode sequences. (CAN-2005-2702)

A bug was found in the way Thunderbird makes XMLHttp requests. It is possible that a malicious HTML mail 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 XMLHttp requests to hosts other than the originator; the default behavior of Thunderbird is to disallow such actions. (CAN-2005-2703)

A bug was found in the way Thunderbird implemented its XBL interface. It may be possible for a malicious HTML mail 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. (CAN-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. (CAN-2005-2705)

A bug was found in the way Thunderbird displays about: pages. It is possible for a malicious HTML mail to open an about: page, such as about:mozilla, in such a way that it becomes possible to execute JavaScript with chrome privileges. (CAN-2005-2706)

A bug was found in the way Thunderbird opens new windows. It is possible for a malicious HTML mail 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. (CAN-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. (CAN-2005-2968)

Users of Thunderbird are advised to upgrade to this updated package, which contains Thunderbird version 1.0.7 and is not vulnerable to these issues.

Patches To Apply :

thunderbird-1.0.7-1.4.1.i386.rpm

Unrated **Moderate: util-linux and mount security update**

BULLETINID :

RHSA-2005:782-01

Description :

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function.

The mount package contains the mount, umount, swapon and swapoff programs.

A bug was found in the way the umount command is executed by normal users. It may be possible for a user to gain elevated privileges if the user is able to execute the 'umount -r' command on a mounted file system. The file system will be re-mounted only with the 'readonly' flag set, clearing flags such as 'nosuid' and 'noexec'. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2876 to this issue.

This update also fixes a hardlink bug in the script command for Red Hat Enterprise Linux 2.1. If a local user places a hardlinked file named 'typescript' in a directory they have write access to, the file will be overwritten if the user running script has write permissions to the destination file. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2001-1494 to this issue.

All users of util-linux and mount should upgrade to these updated packages, which contain backported patches to correct these issues.

Patches To Apply :

util-linux-2.12a-16.EL4.12.i386.rpm

Unrated **Important: wget security update**

BULLETINID :

RHSA-2005:812-00

Description :

GNU Wget is a file retrieval utility that can use either the HTTP or FTP protocols.

A stack based buffer overflow bug was found in the wget implementation of NTLM authentication. An attacker could execute arbitrary code on a user's machine if the user can be tricked into connecting to a malicious web server using NTLM authentication. The Common Vulnerabilities and Exposures project has assigned the name CVE-2005-3185 to this issue.

All users of wget are advised to upgrade to these updated packages, which contain a backported patch that resolves this issue.

Patches To Apply :

wget-1.10.2-0.40E.i386.rpm

Unrated **Low: xloadimage security update**

BULLETINID :

RHSA-2005:802-01

Description :

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).

A flaw was discovered in xloadimage via which an attacker can construct a NIFF image with a very long embedded image title. This image can cause a buffer overflow. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-3178 to this issue.

All users of xloadimage should upgrade to this erratum package, which contains backported patches to correct these issues.

Patches To Apply :

xloadimage-4.1-36.RHEL4.i386.rpm