Insecurity News

wget

In a typical file transfer operation, one participant (the client) requests a file while a second participant (the server) provides the requested file.

Before processing each request, many server implementations will consult an access control policy to determine whether the client should be permitted to read, write, or create a file at the requested location. If the client is able to craft a request that violates the server's access control policy, then the server contains a vulnerability. Since most vulnerabilities of this type involve escaping a restricted set of directories, they are commonly known as "directory traversal" vulnerabilities.

Directory traversal vulnerabilities are most often reported in server implementations, but recent research into the behavior of FTP clients has revealed vulnerabilities in several file transfer applications, including the *wget* utility.

To exploit these vulnerabilities, an attacker must convince the victimized user to access a specific FTP server containing files with crafted filenames. When an affected version of *wget* attempts to download one of these files, the crafted filename causes the utility to write the downloaded files to the location specified by the filename, not by the victim user. In some cases, the attacker must use a modified FTP server to allow the crafted filenames to be passed to the client.

CERT reference VU#210148

Xpdf

Updated Xpdf packages are now available that fix a vulnerability in which a maliciously-crafted pdf document could run arbitrary code.

During an audit of CUPS, a printing system, Zen Parsec found an integer overflow vulnerability in the pdftops filter. Since the code for pdftops is taken from the Xpdf project, all versions of Xpdf including 2.01 are also vulnerable to this issue. An attacker could create a PDF file that could execute arbitrary code. This could would have the same access privileges as the user who viewed the file with Xpdf.

Red Hat reference RHSA-2003:037-09

Security Posture of Major Distributions

Distributor	Security Sources	Comment
Debian	Info: *www.debian.org/security/*, List: debian-security-announce, Reference: DSA-... [1]	Debian have integrated current security advisories on their web site. The advisories take the form of HTML pages with links to patches. The security page also contains a note on the mailing list.
Mandrake	Info: *www.mandrakesecure.net*, List: security-announce, Reference: MDKSA-... [1]	MandrakeSoft run a web site dedicated to security topics. Amongst other things the site contains security advisories and references to mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *www.redhat.com/errata/* List: *www.redhat.com/mailing-lists/* (linux-security and redhat-announce-list) Reference: RHSA-... [1]	Red Hat categorizes security advisories as Errata: Under the Errata headline any and all issues for individual Red Hat Linux versions are grouped and discussed. The security advisories take the form of HTML pages with links to patches.
SCO	Info: *www.sco.com/support/security/*, List: *www.sco.com/support/forums/announce.html*, Reference: CSSA-... [1]	You can access the SCO security page via the support area. The advisories are provided in clear text format.
Slackware	List: *www.slackware.com/lists/* (slackware-security), Reference: slackware-security ... [1]	Slackware do not have their own security page, but do offer an archive of the Security mailing List.
SuSE	Info: *www.suse.de/uk/private/support/security/*, Patches: *www.suse.de/uk/private/download/updates/*, List: suse-security-announce, Reference: suse-security-announce ... [1]	There is a link to the security page on the homepage. The security page contains information on the mailing list and advisories in text format. Security patches for individual SuSE Linux versions are marked red on the general update page and comprise a short description of the patched vulnerability.

[1] Security mails are available from all the above-mentioned distributions via the reference provided.

w3m

New w3m packages are available that fix two cross-site scripting issues.

An XSS vulnerability in w3m 0.3.2 allows remote attackers to insert arbitrary HTML and web script into frames. Frames are disabled by default in the version of w3m shipped with Red Hat Linux. Therefore, this problem will not appear as long as users do not use w3m with the -F option, or enable frame support in either the */etc/w3m/w3mconfig* or *~/.w3m/config* configuration files. The Common Vulnerabilities and Exposures project (*cve.mitre.org*) has assigned the name CAN-2002-1335 to this issue.

An XSS vulnerability in versions of w3m before 0.3.2.2 allows attackers to insert arbitrary HTML and web script into image attributes. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2002-1348 to this issue

Red Hat reference RHSA-2003:044-20

PHP

Updated PHP packages are available that fix a vulnerability in the wordwrap() function and a number of compatibility bugs.

A heap-based buffer overflow was found in the wordwrap() function in PHP versions after 4.1.2 and before 4.3.0. If wordwrap() is used on user-supplied input this could allow remote attackers to cause a denial of service or execute arbitrary code.

Red Hat reference RHSA-2003:017-06

geneweb

A security issue has been discovered by Daniel de Rauglaudre, upstream author of geneweb, a genealogical software with web interface. It runs as a daemon on port 2317 by default.

Paths are not properly sanitized, so a carefully crafted URL can lead geneweb to read and display arbitrary files of the system it runs on.

Debian reference DSA-223-1 geneweb

courier-ssl

The developers of courier, an integrated user side mail server, discovered a problem in the PostgreSQL auth module. Not all potentially malicious characters were

sanitized before the username was passed to the PostgreSQL engine. An attacker could inject arbitrary SQL commands and queries exploiting this vulnerability. The MySQL auth module is not affected.

Debian reference DSA-247-1 courier-ssl

bugzilla

Two vulnerabilities have been discovered in Bugzilla, a web-based bug tracking system, by its authors. The Common Vulnerabilities and Exposures Project identifies the following vulnerabilities:

CAN-2003-0012 (BugTraq ID 6502)

The provided data collection script intended to be run as a nightly cron job changes the permissions of the data/mining directory to be world-writable every time it runs. This would enable local users to alter or delete the collected data.

CAN-2003-0013 (BugTraq ID 6501)

The default .htaccess scripts provided by checksetup.pl do not block access to backups of the localconfig file that might be created by editors such as vi or emacs (typically these will have a .swp or ~ suffix). This allows an end user to download one of the backup copies and potentially obtain your database password.

This does not affect the Debian installation because there is no .htaccess as all data file aren't under the CGI path as they are on the standard Bugzilla package. Additionally, the configuration is in */etc/bugzilla/localconfig* and hence outside of the web directory.

Debian reference DSA-230-1 bugzilla

dhcp3

Florian Lohoff discovered a bug in the dhcrelay causing it to send a continuing packet storm towards the configured DHCP server(s) in case of a malicious BOOTP packet, such as sent from buggy Cisco switches.

When the dhcp-relay receives a BOOTP request it forwards the request to the DHCP server using the broadcast MAC address ff:ff:ff:ff:ff:ff which causes the network interface to reflect the packet back into the socket. To prevent loops the dhcrelay checks whether the relay-address is its own, in which case the packet would be dropped. In combination with a missing upper boundary for the hop counter an attacker can force the dhcp-relay to send a continuing packet storm towards the configured dhcp server(s).

This patch introduces a new command line switch *-c maxcount* and people are advised to start the dhcp-relay with *dhcrelay -c 10* or a smaller number, which will only create that many packets.

The dhcrelay program from the "dhcp" package does not seem to be affected since DHCP packets are dropped if they were apparently relayed already.

Debian reference DSA-245-1 dhcp3

cvs

Stefan Esser discovered a problem in cvs, a concurrent versions system, which is used for many Free Software projects. The current version contains a flaw that can be used by a remote attacker to execute arbitrary code on the CVS server under the user id the CVS server runs as. Anonymous read-only access is sufficient to exploit this problem.

Debian reference DSA-233-1 cvs

libpng

A buffer overflow vulnerability was discovered in libpng due to a wrong calculation of some loop offset values. This buffer overflow can lead to Denial of Service or even remote compromise.

After the upgrade, all applications that use libpng should be restarted. Many applications are linked to libpng, so if you are unsure of what applications to restart, you may wish to reboot the system.

Mandrake reference MDKSA-2003:008 : libpng

MySQL

Aleksander Adamowski informed MandrakeSoft that the MySQL developers fixed a DoS vulnerability in the recently released 3.23.55 version of MySQL.

A double free() pointer bug in the mysql_change_user() handling would allow a specially hacked mysql client to crash the main mysqld server. This vulnerability can only be exploited by first logging in with a valid user account.

Mandrake reference MDKSA-2003:013 : MYSQL

printer-drivers

Karol Wiesek and iDefense disovered three vulnerabilities in the printer-drivers package and tools it installs. These vulnerabilities allow a local attacker to empty or create any file on the filesystem.

The first vulnerability is in the mtink binary, which has a buffer overflow in its handling of the HOME environment variable.

The second vulnerability is in the escputil binary, which has a buffer overflow in the parsing of the --printer-name command line argument. This is only possible when esputil is suid or sgid; in Mandrake Linux 9.0 it was sgid "sys". Successful exploitation will provide the attacker with the privilege of the group "sys".

The third vulnerability is in the ml85p binary which contains a race condition in the opening of a temporary file. By default this file is installed suid root so it can be used to gain root privilege. The only caveat is that this file is not executable by others , only by root or group "sys". Using either of the two previous vulnerabilities, an attacker can exploit one of them to obtain "sys" privilege" and then use that to exploit this vulnerability to gain root privilege.

Mandrake reference MDKSA-2003:010 : printer-drivers

SuSEhelp

During a code review of the susehelp package the SuSE Security Team recognized that the security checks done by the susehelp CGI scripts are insufficient. Remote attackers can insert certain characters in CGI queries to the susehelp system tricking it into executing arbitrary code as the "wwwrun" user.

Please note that this is only a vulnerability if you have a web server running and configured to allow access to the susehelp system by remote sites. We nevertheless recommend an update of this package. As a temporary workaround you may un-install the susehelp package by issuing the following command as root:

```
rpm -e --nodeps susehelp
```

SuSE reference SuSE-SA:2003:005