Insecurity News

Dvips

dvips contains a flaw allowing print users to execute arbitrary commands. The dvips utility converts DVI format into PostScript(TM), and is used in Red Hat Linux as a print filter for printing DVI files. A vulnerability has been found in dvips which uses the system() function insecurely when managing fonts. Since dvips is used in a print filter, this allows local or remote attackers who have print access to craft carefully a print job that would allow them to execute arbitrary code as the user 'lp'. A work around for this vulnerability is to remove the print filter for DVI files. The following commands, run as root, will accomplish this: rm -f /usr/share /printconf/mf_ rules/ mf40-tetex_filters rm -f /usr/lib/rhs/ rhs-printfilters/dvi-to-ps.fpi However, to fix the problem in the dvips utility as well as removing the print filter we recommend that all users upgrade these errata packages. This vulnerability was discovered by Olaf Kirch of SuSE. Additionally, the file /var/lib/ texmf/ls-R had world-writable permissions. ■

Red Hat reference RHSA-2002-192-18

Mozilla

Updated Mozilla packages are now available for Red Hat Linux. These new packages fix vulnerabilities in previous versions of Mozilla. Mozilla is an open source web browser. Versions of Mozilla previous to version 1.0.1 contain various security vulnerabilities. These security flaws could be used by an attacker to read data off the local hard drive, to gain information that should normally be kept private, and in some cases to execute arbitrary code. All users of Mozilla should update to packages containing Mozilla version 1.0.1 which is not vulnerable to these issues. ■

Red Hat reference RHSA-2002-192-13

bugzilla

The developers of Bugzilla, a web-based bug tracking system, discovered a problem in the handling of more than 47 groups. When a new product is added to an installation with 47 groups or more and "usebuggroups" is enabled, the new group will be assigned a groupset bit using Perl math that is not exact beyond 2^48. This results in the new group being defined with a "bit" that has several bits set.

As users are given access to the new group, those users will also gain access to spurious lower group privileges. Also, group bits were not always reused when groups were deleted.

This problem has been fixed in version 2.14.2-0woody2 for the current stable distribution (woody) and will soon be fixed in the unstable distribution (sid). ■

Debian reference DSA-173-1

pam

Paul Aurich and Samuele Giovanni Tonon discovered a serious security violation in PAM. Disabled passwords (i.e. those with '*' in the password file) were classified as empty password and access to such accounts is granted through the regular login procedure (getty, telnet, ssh). This works for all such accounts whose shell field in the password file does not refer to /bin/false. Only version 0.76 of PAM seems to be affected by this problem.

This problem has been fixed in version 0.76-6 for the current unstable distribution (sid). The stable distribution (woody), the old stable distribution (potato) and the testing distribution (sarge) are not affected by this problem. ■

Debian reference DSA-177-1

tkmail

It has been discovered that tkmail creates temporary files insecurely. Exploiting this an attacker with local access can create and overwrite files as another user. This has been fixed in version 4.0beta9-8.1 for the current stable distribution (woody), in version 4.0beta9-4.1 for the old stable distribution (potato) and in version 4.0beta9-9 for the unstable distribution (sid) of Debian. ■

Debian reference DSA-172-1

Heartbeat

Heartbeat is a monitoring service that is used to implement failover in high-availablity environments. It can be configured to monitor other systems via serial connections, or via UDP/IP.

Several format string bugs have been discovered in the Heartbeat package. One of these format string bugs is in the normal path of execution, all the remaining ones can only be triggered if Heartbeat is running in debug mode.

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.

Since Heartbeat is running with root privilege, this problem can possibly be exploited by remote attackers, provided they are able to send packets to the UDP port Heartbeat is listening on (port 694 by default).

Vulnerable versions of Heartbeat are included in SuSE Linux 8.0 and SuSE Linux 8.1. As a workaround, make sure that your firewall blocks all traffic to the Heartbeat UDP port.

SuSE reference SuSE-SA:2002:037

HylaFAX

HylaFAX is a client-server architecture for receiving and sending facsimiles. The logging function of faxgetty prior version 4.1.3 was vulnerable to a format string bug when handling the TSI value of a received facsimile. This bug could be used to trigger a denial-of-service attack or to execute arbitrary code remotely.

Another bug in faxgetty, a buffer overflow, can be abused by a remote attacker by sending a large line of image data to execute arbitrary commands too. Several format string bugs in local helper applications were fixed too. These bugs can not be exploited to gain higher privileges on a system running SuSE Linux because of the absence of setuid bits. The hylafax package is not installed by default. A temporary fix is not known. Please download the update package for your distribution. Then, install the package using the usual rpm command "rpm -Fhv file.rpm" to apply the update.

SuSE reference SuSE-SA:2002:035

apache

A number of vulnerabilities were discovered in Apache versions prior to 1.3.27. The first is regarding the use of shared memory (SHM) in Apache. An attacker who is able to execute code as the UID of the webserver (typically "apache") is able to send arbitrary processes a USR1 signal as root.

Using this vulnerability, the attacker can also cause the Apache process to spawn continuously more children processes, thus causing a local DoS. Another vulnerability was discovered by Matthew Murphy regarding a cross site scripting vulnerability in the standard 404 error page. Finally, some buffer overflows were found in the "ab" benchmark program that is included with Apache. All of these vulnerabilities were fixed in Apache 1.3.27.

Mandrake reference MDKSA-2002:068

drakconf

Errors were discovered in the Mandrake Control Center that prevents any users using the nl_NL, sl, and zh_CN locales from starting the program. The error generated would be shown as "cannot call set_active on undefined values" on line 423.

Mandrake reference MDKA-2002:012

tar

A directory traversal vulnerability was discovered in GNU tar version 1.13.25 and earlier that allows attackers to overwrite arbitrary files during extraction of the archive by using a ".." (dot dot) in an extracted filename.

Mandrake reference MDKSA-2002:066