Insecurity News

XFree86

XFree86 is an implementation of the X Window System providing the core graphical user interface and video drivers. XDM is the X display manager.

Multiple integer overflows in the transfer and enumeration of font libraries in XFree86 allow local or remote attackers to cause a denial of service or execute arbitrary code via heap-based and stack-based buffer overflow attacks. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0730 to this issue.

The risk to users from this vulnerability is limited because only clients can be affected by these bugs, however in some (non-default) configurations, both xfs and the X Server can act as clients to remote font servers.

XDM does not verify whether the pam_setcred function call succeeds, which may allow attackers to gain root privileges by triggering error conditions within PAM modules, as demonstrated in certain configurations of the pam_krb5 module. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0690 to this issue.

XDM uses a weak session cookie generation algorithm that does not provide 128 bits of entropy, which allows attackers to guess session cookies via brute force methods and gain access to the user session. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0692 to this issue.

Red Hat reference RHSA-2003:288-05

Zebra

Jonny Robertson reported that Zebra, an implementation of TCP/IP routing, can be remotely crashed if a Zebra password has been enabled and an attacker can connect to the Zebra telnet management port. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0795 to this issue.

Red Hat reference RHSA-2003:307-09

Security Posture of Major Distributions

Distributor	Security Sources	Comments
Debian	Info: *http://www.debian.org/security/* List: *http://lists.debian.org/debian-security-announce/* Reference: DSA-... 1)	The current Debian security advisories are included on the homepage. Advisories are provided as HTML pages with links to the patches. The security advisory also contains a reference to the mailing list.
Gentoo	Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	Unfortunately, Gentoo does not offer a website with security updates or other security information. This forum is the only alternative.
Mandrake	Info: *http://www.mandrakesecure.net* List: *http://www.mandrakesecure.net/en/mlist.php* Reference: MDKSA-... 1)	MandrakeSoft runs its own Web site on security topics. Among other things, it includes security advisories and references to the mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *http://www.redhat.com/errata/* List: *http://www.redhat.com/mailing-lists/* Reference: RHSA-... 1)	Red Hat files security advisories as so-called Errata: Issues for each Red Hat Linux version are then grouped. The security advisories are provided in the form of an HTML page with links to patches.
Slackware	Info: *http://www.slackware.com/security/* List: *http://www.slackware.com/lists/* (slackware-security) Reference: [slackware-security] ... 1)	The start page contains links to the security mailing list archive. No additional information on Slackware security is available.
Suse	Info: *http://www.suse.de/uk/private/support/security/* Patches: *http://www.suse.de/uk/private/download/updates/* List: suse-security-announce Reference: SUSE-SA ... 1)	There is no longer a link to the security page after changes to the Web site. It contains information on the mailing list and the advisories. The security patches for the individual Suse Linux versions are shown in red on the general updates site. A short description of the vulnerability the patch resolves is provided

1) All distributors indicate security mails in the subject line.

Pan

Pan is a Gnome/GTK+ newsreader. Kasper Dupont discovered a bug in Pan versions prior to 0.13.4 that can cause Pan to crash when parsing an article header containing a very long author email address. This bug causes a crash (denial of service) but is not otherwise exploitable. Charles Kerr has produced a patch. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0855 to this issue.

Red Hat reference RHSA-2003:311-06

EPIC

EPIC (Enhanced Programmable ircII Client) is an advanced ircII chat client designed to connect to Internet Relay Chat (IRC) servers.

A bug in various versions of EPIC allows remote malicious IRC servers to cause a denial of service (crash) and execute arbitrary code via a CTCP request from a large nickname, which causes an incorrect length calculation. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0328 to this issue.

Red Hat reference RHSA-2003:342-05

glibc

glibc packages contain GNU libc, which provides standard system libraries.

A vulnerability in the getgrouplist function can cause a buffer overflow if the size of the group list is too small to hold all the user's groups. This overflow can cause segmentation faults in user applications, which may have security implications. This vulnerability exists only when an administrator has placed a user in a number of groups larger than that expected by an application. Therefore, there is no risk in instances where users are members of few groups. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0689 to this issue.

Herbert Xu reported that various applications can accept spoofed messages sent on the kernel netlink interface by other users on the local machine. This could lead to a local denial of service attack. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0859 to this issue.

Red Hat reference RHSA-2003:325-10

Linux Kernel

A flaw in bounds checking in the do_brk() function in the Linux kernel versions 2.4.22 and previous can allow a local attacker to gain root privileges. This issue is known to be exploitable; an exploit has been seen in the wild. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0961 to this issue. ■

Red Hat reference RHSA-2003:392-05
SUSE reference SuSE-SA:2003:049

Net-SNMP

The Net-SNMP project includes various Simple Network Management Protocol (SNMP) tools.

A bug in Net-SNMP version 5.0.9 could allow an existing user/community to gain access to data in MIB objects that were explicitly excluded from their view. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0935 to this issue. ■

Red Hat reference RHSA-2003:335-07
Mandrake reference MDKSA-2003:115

Debian Compromised

The Debian project has issued the following announcement:

> "Some Debian Project machines compromised November 21st, 2003.
>
> This is a very unfortunate incident to report about. Some Debian servers were found to have been compromised in the last 24 hours. The archive is not affected by this compromise!
>
> In particular the following machines have been affected:
>
> - master (Bug Tracking System)
> - murphy (mailing lists)
> - gluck (web, cvs, people)
> - klecker (security, non-us, web search, www-master, qa)
>
> Some of these services are currently not available while the machines undergo close inspection. Some services have been moved to other machines (*http://www.debian.org* for example).
>
> The security archive will be verified from trusted sources before it becomes available again. Please note that we have recently prepared a new point release for Debian GNU/Linux 3.0 (*woody*), release 3.0r2. While it has not been announced yet, it has been pushed to our mirrors already. The announcement was scheduled for this morning but had to be postponed. This update has now been checked and it is not affected by the compromise.
>
> We apologise for the disruptions of some services over the next few days. We are working on restoring the services and verifying the content of our archives." ■

Minimalist

A security-related problem has been discovered in minimalist, a mailing list manager, which allows a remote attacker to execute arbitrary commands.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0902 to this issue. ■

Debian reference DSA-402-1 minimalist – unsanitised input