Insecurity News

Sendmail

Michal Zalewski discovered a buffer overflow, triggered by a char to int conversion, in the address parsing code in sendmail, a widely used powerful, efficient, and scalable mail transport agent. This problem is potentially remotely exploitable.

Debian reference DSA-278-1 sendmail – char-to-int conversion

Samba

Sebastian Krahmer of the SuSE security audit team found two problems in Samba, a popular SMB/CIFS implementation. The problems are a buffer overflow in the SMB/CIFS packet fragment re-assembly code used by smbd. Since smbd runs as root an attacker can use this to gain root access to a machine running smbd.

The second problem is the code to write reg files was vulnerable for a chown race which made it possible for a local user to overwrite system files.

Debian reference DSA-262-1 samba – remote exploit

Lxr

Upstream developers of lxr, a general hypertext cross-referencing tool, have been alerted of a vulnerability that allows a remote attacker to read arbitrary files on the host system as user www-data. This could disclose local files that were not meant to be shared with the public.

Debian reference DSA-264-1 lxr – missing filename sanitizing

Tcpdump

A problem has been discovered in tcpdump, a powerful tool for network monitoring and data acquisition. An attacker is able to send a specially crafted RADIUS network packet which causes tcpdump to enter an infinite loop.

Debian reference DSA-261-1 tcpdump – infinite loop

Qpopper

Florian Heinz posted to the Bugtraq mailing list an exploit for qpopper based on a bug in the included vsnprintf implementation. The sample exploit requires a valid user account and password, and overflows a string in the pop_msg() function to give the user "mail" group privileges and a shell on the system. Since the Qvsnprintf function is used elsewhere in qpopper, additional exploits may be possible.

Debian reference DSA-259-1 qpopper – mail user privilege escalation

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.

krb4

A cryptographic weakness in version 4 of the Kerberos protocol allows an attacker to use a chosen-plaintext attack to impersonate any principal in a realm.

Additional cryptographic weaknesses in the krb4 implementation permit the use of cut-and-paste attacks to fabricate krb4 tickets for unauthorized client principals if triple-DES keys are used to key krb4 services. These attacks can subvert a site's entire Kerberos authentication infrastructure.

Debian reference DSA-273-1 krb4 – Cryptographic weakness

Ecartis

A problem has been discovered in ecartis, a mailing list manager, formerly known as listar. This vulnerability enables an attacker to reset the password of any user defined on the list server, including the list admins.

Debian reference DSA-271-1 ecartis – unauthorized password change

Ethereal

Georgi Guninski discovered a problem in ethereal, a network traffic analyzer. The program contains a format string vulnerability that could probably lead to execution of arbitrary code.

Debian reference DSA-258-1 ethereal – format string vulnerability

Rxvt

Digital Defense Inc. released a paper detailing insecurities in various terminal emulators, including rxvt. Many of the features supported by these programs can be abused when untrustworthy data is displayed on the screen. This abuse can be anything from garbage data being displayed to the screen or a system compromise.

Mandrake reference MDKSA-2003:034-1 : rxvt

Krb5

Multiple vulnerabilities have been found in the Kerberos network authentication system. The MIT Kerberos team have released an advisory detailing these vulnerabilities, a description of which follows:

- An error in the way integers are signed in the ASN.1 decoder before version 1.2.5 allows remote attackers to cause a crash of the server via a large unsigned data element length, which is later used as a negative value (CAN-2002-0036).
- Vulnerabilities have been found in the RPC library used by the kadmin service. A faulty length check in the RPC library exposes kadmind to an integer overflow which can be used to crash kadmind (CAN-2003-0028).
- The KDC (Key Distribution Center) before version 1.2.5 allows remote, authenticated attackers to cause a crash on KDCs within the same realm using a certain protocol that causes a null dereference (CAN-2003-0058).
- Users from one realm can impersonate users in other realms that have the same inter-realm keys due to a vulnerability in Kerberos 1.2.3 and earlier (CAN-2003-0059). Mandrake Linux 9.0+ is not affected by this problem.
- The KDC allows remote, authenticated users, to cause a crash on KDCs within the same realm using a certain protocol request that causes an out-of-bounds read of an array (CAN-2003-0072).
- The KDC allows remote, authenticated users to cause a crash on KDCs within the same realm using a certain protocol request that causes the KDC to corrupt its heap (CAN-2003-0082).
- Vulnerabilities have been discovered in the Kerberos IV authentication protocol which allow an attacker with knowledge of a cross-realm key, which is shared in another realm, to impersonate a principle in that realm to any service in that realm. This vulnerability can only be closed by disabling cross-realm authentication in Kerberos IV (CAN-2003-0138).
- Vulnerabilities have been discovered in the support for triple-DES keys in the Kerberos IV authentication protocol which is included in MIT Kerberos (CAN-2003-0139). ■

Mandrake reference MDKSA-2003:043-1 : krb5

OpenSSL

Researchers discovered a timing-based attack on RSA keys that OpenSSL is generally vulnerable to, unless RSA blinding is enabled. Patches from the OpenSSL team have been applied to turn RSA blinding on by default.

An extension of the "Bleichenbacher attack" on RSA with PKS #1 v1.5 padding as used in SSL 3.0 and TSL 1.0 was also created by Czech cryptologists Vlastimil Klima, Ondrej Pokorny, and Tomas Rosa.

This attack requires the attacker to open millions of SSL/TLS connections to the server they are attacking. This is done because the server's behavior when faced with specially crafted RSA ciphertexts can reveal information that would in effect allow the attacker to perform a single RSA private key operation on a ciphertext of their choice, using the server's RSA key. Despite this, the server's RSA key is not compromised at any time.

Patches from the OpenSSL team modify SSL/TLS server behavior to avoid this vulnerability. ■

Mandrake reference MDKSA-2003:035 : openssl

Eye of GNOME

Eye of GNOME (EOG) is a component for the GNOME desktop used by various Red Hat Linux packages for displaying images.

A vulnerability was found in EOG version 2.2.0 and earlier. A carefully crafted filename passed to the program could lead to the execution of arbitrary code. An attacker could exploit this because various packages (Mutt, for example) make use of EOG for image viewing. ■

Red Hat reference RHSA-2003:128-07

Evolution

Evolution is a GNOME-based collection of personal information management (PIM) tools.Multiple vulnerabilities have been found in the Ximian Evolution email client. These vulnerabilities make it possible for a carefully crafted email to crash the program, cause general system instability through resource starvation, and get around security measures implemented within the program. ■

Red Hat reference RHSA-2003:108-19

Vsftpd

In Red Hat Linux 9, the vsftpd FTP daemon switched from being run by xinetd to being run as a standalone service. In doing so, it was accidentally not compiled against tcp_wrappers.

Users of vsftpd who make use of tcp_wrappers features are advised to upgrade to these errata packages.

This issue only affects Red Hat Linux 9 boxed sets manufactured for distribution within the USA with the part numbers, RHF0120US and RHF0121US (see the bottom flap of the box). ■

Red Hat reference RHSA-2003:084-06

Lprold

The lprm command of the printing package lprold shipped till SuSE 7.3 contains a buffer overflow. This buffer overflow can be exploited by a local user, if the printer system is set up correctly, to gain root privileges. lprold is installed as the default package and has its setuid bit set.

As a temporary workaround you can disable the setuid bit of lprm by executing the following tasks as root:

- add "/usr/bin/lprm root.root 755" to /etc/permissions.local
- run 'chkstat -set /etc/permissions.local'

Another way would be to just allow trusted users to run lprm by executing the following tasks as root:

- add "/usr/bin/lprm root.trusted 4750" to /etc/permissions.local
- run 'chkstat -set /etc/permissions.local' ■

SuSE reference SuSE-SA:2003:0014

Hypermail

Hypermail is a tool to convert a Unix mail-box file to a set of cross-referenced HTML documents.

During an internal source code review done by Thomas Biege several bugs where found in Hypermail and its tools. These bugs allow remote code execution, local /tmp race conditions, denial-of-service conditions and read access to files belonging to the host Hypermail is running on. Additionally the mail CGI program can be abused by spammers as email-relay and should thus be disabled.

There is no temporary fix known other then disabling Hypermail. ■

SuSE reference SuSE-SA:2003:0012