Insecurity News

Lftp

The the flexible and powerful FTP command-line client lftp is vulnerable to two remote buffer overflows discovered by Ulf Harnhammar .

When using lftp via HTTP or HTTPS to execute commands like 'ls' or 'rels' specially prepared directories on the server can trigger a buffer overflow in the HTTP handling functions of lftp to possibly execute arbitrary code on the client-side.

Please note, to exploit these bugs an attacker has to control the server-side of the context and the attacker will only gain access to the account of the user that is executing lftp.

This vulnerability exists in lftp versions 2.3.0 through 2.6.9 and is corrected upstream in 2.6.10.

Suse reference SuSE-SA:2003:051
Mandrake reference MDKSA-2003:116 : lftp
Red Hat reference RHSA-2003:403-07
Debian reference DSA-406-1 lftp – buffer overflow

Kernel 2.4.23 and previous

The do_mremap() function of the Linux Kernel is used to manage (move, resize) Virtual Memory Areas (VMAs). By exploiting an incorrect bounds check, discovered by Paul Starzetz, in do_mremap() during the remapping of memory it is possible to create a VMA with the size of 0.

In normal operation do_mremap() leaves a memory hole of one page and creates an additional VMA of two pages. In the case of exploitation no hole is created, but the new VMA has a 0 bytes length.

The Linux Kernel's memory management is corrupted from this point and can in turn be abused by any local users to gain root privileges and so compromise the system.

Version 2.2 is not affected by this bug.

Suse reference SuSE-SA:2004:001
Mandrake reference MDKSA-2004:001 : kernel
Red Hat reference RHSA-2003:417-08

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.

irssi

A vulnerability in versions of irssi prior to 0.8.9 would allow a remote user to crash another user's irssi client provided that the client was on a non-x86 architecture or if the "gui print text" signal is being used by some script or plugin.

Mandrake reference MDKSA-2003:117 : irssi

Ethereal

Ethereal is a program for monitoring network traffic.

Two security issues have been found that affect Ethereal. By exploiting these issues it may be possible to make Ethereal crash by injecting an intentionally malformed packet onto the wire or by convincing someone to read a malformed packet trace file. It is not known if these issues could allow arbitrary code execution.

The SMB dissector in Ethereal before 0.10.0 allows remote attackers to cause a denial of service via a malformed SMB packet that triggers a segmentation fault during processing of selected packets. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-1012 to this issue.

The Q.931 dissector in Ethereal before 0.10.0 allows remote attackers to cause a denial of service (crash) via a malformed Q.931, which triggers a null dereference. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-1013 to this issue.

Red Hat reference RHSA-2004:001-03
Debian reference DSA-407-1 ethereal – buffer overflows

CVS

CVS is a version control system frequently used to manage source code repositories.

A flaw was found in versions of CVS prior to 1.11.10 where a malformed module request could cause the CVS server to attempt to create files or directories at the root level of the file system.

However, normal file system permissions would prevent the creation of these misplaced directories. The Common Vulnerabilities and Exposures project has assigned the name CAN-2003-0977 to this issue.

Red Hat reference RHSA-2004:003-04

httpd

The Apache HTTP Server is a powerful, full-featured, efficient Web server.

An issue in the handling of regular expressions from configuration files was discovered in releases of the Apache HTTP Server version 2.0 prior to 2.0.48. An attacker would need to have the ability to write to Apache configuration files such as .htaccess or httpd.conf.

A carefully-crafted configuration file can cause an exploitable buffer overflow and would allow the attacker to execute arbitrary code in the context of the server (in default configurations as the 'apache' user).

A bug in the CGI daemon-based "mod_cgid" module was discovered that can result in CGI script output being sent to the wrong client.

This issue only affects servers configured to use the "worker" MPM. The default configuration uses the "mod_cgi" module for CGI and is not affected by this issue.

Red Hat reference RHSA-2003:320-09

phpgroupware

The authors of phpgroupware, a Web-based groupware system written in PHP, discovered several vulnerabilities. The Common Vulnerabilities and Exposures project identifies the following problems:

CAN-2004-0016 – In the "calendar" module, "save extension" was not enforced for holiday files. As a result, server-side php scripts may be placed in directories that then could be accessed remotely and cause the webserver to execute those. This was resolved by enforcing the extension ".txt" for holiday files.

CAN-2004-0017 – Some SQL injection problems (non-escaping of values used in SQL strings) the "calendar" and "infolog" modules.

Additionally, the Debian maintainer adjusted the permissions on world writable directories that were accidentally created by former postinst during the installation.

Debian reference DSA-419-1 phpgroupware – missing filename sanitizing, SQL injection

vbox3

A bug was discovered in vbox3, a voice response system for isdn4linux, whereby root privileges were not properly relinquished before executing a user-supplied tcl script. By exploiting this vulnerability, a local user could gain root privileges.

Debian reference DSA-418-1 vbox3 – privilege leak

jitterbug

Steve Kemp discovered a security related problem in jitterbug, a simple CGI based bug tracking and reporting tool. Unfortunately program executions do not use properly sanitized input, which allows an attacker to execute arbitrary commands on the server hosting the bug database. As a mitigating factor, these attacks are only available to non-guest users, and accounts for these people must be set up by the administrator making them "trusted".

Debian reference DSA-420-1 jitterbug – improperly sanitized input