MOZILLA

Mozilla is an open source Web browser, advanced email and newsgroup client, IRC chat client, and HTML editor.

Several bugs were found in the way Mozilla executes javascript code. Javascript executed from a web page should run with a restricted access level, preventing dangerous actions. It is possible that a malicious web page could execute javascript code with elevated privileges, allowing access to protected data and functions. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-1476, CAN-2005-1477, CAN-2005-1531, and CAN-2005-1532 to these issues.

Users of Mozilla are advised to upgrade to the latest version, which contains corrections for these problems.

Gentoo reference:GLSA 200505-11 / mozilla
Red Hat reference:RHSA-2005:434-10; RHSA-2005:435-14
Slackware reference:SSA:2005-135-01
Suse reference:SUSE-SA:2005:030

GZIP

gzip is a file compression tool.

Zgrep in gzip before 1.3.5 does not properly sanitize arguments, which allows local users to execute arbitrary commands via filenames that are injected into a sed script. (CAN-2005-0758)

A race condition in gzip 1.2.4, 1.3.3, and earlier when decompressing a gzip file allows local users to modify permissions of arbitrary files via a hard link attack on a file while it is being decompressed. (CAN-2005-0988)

A directory traversal vulnerability via "gunzip -N" in gzip 1.2.4 through 1.3.5 allows remote attackers to write to arbitrary directories via a .. (dot dot) in the original filename within a compressed file. (CAN-2005-1228)

Updated packages are patched to address these issues.

Gentoo reference:GLSA 200505-05 / gzip
Mandriva reference:MDKSA-2005:092
Red Hat reference:RHSA-2005:357-19

GEDIT

gEdit is a small text editor designed specifically for the GNOME GUI desktop environment.

A file name format string vulnerability has been discovered in gEdit. It is possible for an attacker to create a file with a carefully crafted name which, when the file is opened, executes arbitrary instructions on a victim's machine. Although it is unlikely that a user would manually open a file with such a carefully crafted file name, there are situation where a user could be tricked into opening the file; for example, the user may open such a file from within an email client. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1686 to this issue.

Users of gEdit should upgrade to this updated package, which contains a backported patch to correct this issue.

Gentoo reference:GLSA 200506-09 / gedit
Red Hat reference:RHSA-2005:499-05