and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0232 to this issue.

A bug was found in the way Mozilla Mail handles cookies when loading content over HTTP regardless of the user's preference. It is possible that a particular user could be tracked through the use of malicious mail messages which load content over HTTP. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0149 to this issue.

A bug was found in the way Mozilla responds to proxy auth requests. It is possible for a malicious webserver to steal credentials from a victim's browser by issuing a 407 proxy authentication request. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0147 to this issue.

A bug was found in the way Mozilla handles certain start tags followed by a NULL character. A malicious web page could cause Mozilla to crash when viewed by a victim. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-1613 to this issue.

A bug was found in the way Mozilla sets file permissions when installing XPI packages. It is possible for an XPI package to install some files world readable or writable, allowing a malicious local user to steal information or execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0906 to this issue.

A bug was found in the way Mozilla loads links which are middle clicked in a new tab. A malicious web page could read local files or modify privileged chrom settings. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0141 to this issue.

A bug was found in the way Mozilla displays the secure site icon. A malicious web page can use a view-source URL targetted at a secure page, while loading an insecure page, yet the secure site icon shows the previous secure state. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0144 to this issue.

Gentoo reference: GLSA 200503-30 / Mozilla

Red Hat reference: RHSA-2005:323-10

GTK2

The gtk2 package contains the GIMP ToolKit (GTK+), a library for creating graphical user interfaces for the X Window System.

A bug was found in the way gtk2 processes BMP images. It is possible that a specially crafted BMP image could cause a denial of service attack on applications linked against gtk2.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0891 to this issue.

Mandriva reference: MDKSA-2005:068

Red Hat reference: RHSA-2005:344-03