FIREFOX

Mozilla Firefox is an open source Web browser.

Vladimir V. Perepelitsa discovered a bug in the way Firefox handles anonymous functions during regular expression string replacement. It is possible for a malicious web page to capture a random block of browser memory. The CVE project has assigned the name CAN-2005-0989 to this issue.

Omar Khan discovered a bug in the way Firefox processes the PLUGINSPAGE tag. A malicious web page can trick a user into pressing the "manual install" button for an unknown plugin. The CVE project has assigned the name CAN-2005-0752 to this issue.

Doron Rosenberg discovered a bug in the way Firefox displays pop-up windows. If a user chooses to open a pop-up window whose URL is malicious javascript, the script will be executed with elevated privileges. The CVE project has assigned the name CAN-2005-1153 to this issue.

A bug was found in the way Firefox handles the javascript global scope for a window. A malicious web page can define a global variable known to be used by a different site, allowing malicious code to be executed in the context of the site. The CVE project has assigned the name CAN-2005-1154 to this issue.

Michael Krax discovered a bug in the way Firefox handles favicon links. A malicious web page can define a favicon link tag as javascript, executing arbitrary javascript with elevated privileges. The CVE project has assigned the name CAN-2005-1155 to this issue.

Michael Krax discovered a bug in the way Firefox installs search plugins. If a user chooses to install a search plugin from a malicious site, the new plugin could silently overwrite an existing plugin. The CVE project has assigned the names CAN-2005-1156 and CAN-2005-1157 to these issues.

Kohei Yoshino discovered a bug in the way Firefox opens links in its sidebar. A malicious web page could construct a link in such a way that, when clicked on, it could execute arbitrary javascript with elevated privileges. The CVE project has assigned the name CAN-2005-1158 to this issue.

A bug was found in the way Firefox validates several XPInstall related javascript objects. A malicious web page could pass other objects to the XPInstall objects, resulting in the javascript interpreter jumping to arbitrary locations in memory. The CVE project has assigned the name CAN-2005-1159 to this issue.

A bug was found in the way the privileged UI code handles DOM nodes. A malicious web page could install malicious javascript code or steal data. The CVE project has assigned the name CAN-2005-1160 to this issue.

Gentoo reference: GLSA 200504-18 / Mozilla; GLSA 200505-11 / mozilla
Mandriva reference: MDKSA-2005:088
Red Hat reference: RHSA-2005:383-07
Slackware reference: SSA:2005-111-04; SSA:2005-135-01
Suse reference: SUSE-SA:2005:028