

13 July 2005

By:



[Mozilla Foundation Releases Firefox 1.0.5](#)

Which fixes 12 bugs

Yesterday, Mozilla Foundation released version 1.0.5 of its famous Firefox browser which patches 12 security bugs, two of which being rated as critical. One of these bugs refers to the capability of standalone applications to run arbitrary code through the browser. Several media players, for example Flash and QuickTime, support scripted content with the ability to open URLs in the default browser. The default behavior for Firefox was to replace the currently open browser window's content with the externally opened content. If the external URL was a javascript: url it would run as if it came from the site that served the previous content, which could be used to steal sensitive information such as login cookies or passwords. If the media player content first caused a privileged chrome: url to load then the subsequent javascript: url could execute arbitrary code. External javascript: urls will now run in a blank context regardless of what content it's replacing, and external apps will no longer be able to load privileged chrome: urls in a browser window. The -chrome command line option to load chrome applications is still supported. The other critical bug refers to the code execution through shared function objects. Improper cloning of base objects allowed web content scripts to walk up the prototype chain to get to a privileged object. This could be used to execute code with enhanced privileges. The new version solves four more bugs, rated as "high": Content-generated event vulnerabilities, Code execution via "Set as Wallpaper", Script injection from Firefox sidebar panel using data: and XHTML node spoofing. The remaining bugs are rated as "moderate" and "low" and don't pose a grave threat to the users' security.