Mozilla Firefox Two Vulnerabilities

By *srlinuxx*
Created *08/05/2005 - 4:44pm*
Submitted by srlinuxx on Sunday 8th of May 2005 04:44:03 PM Filed under Security [1]

Classified **Extremely critical**, two vulnerabilities have been discovered in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system.

Description:
Two vulnerabilities have been discovered in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system.

1) The problem is that "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site.

2) Input passed to the "IconURL" parameter in "InstallTrigger.install()" is not properly verified before being used. This can be exploited to execute arbitrary JavaScript code with escalated privileges via a specially crafted JavaScript URL.

Successful exploitation requires that the site is allowed to install software (default sites are "update.mozilla.org" and "addons.mozilla.org").

A combination of vulnerability 1 and 2 can be exploited to execute arbitrary code.

NOTE: Exploit code is publicly available.

The vulnerabilities have been confirmed in version 1.0.3. Other versions may also be affected.

Solution:
Disable JavaScript.

Linkage [2].

Security

Source URL: http://www.tuxmachines.org/node/872

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://secunia.com/advisories/15292/