

Firesearching 1 + 2 [Firefox 1.0.2]

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0052.html>

From: mikx (*mikx_at_MIKX.DE*)

Date: 04/18/05

Date: Mon, 18 Apr 2005 12:58:33 +0200

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

__Notice

I really wonder why the Mozilla Foundation decided to release a serious security update on a friday night and to disclose the link to my proof-of-concept code so quickly. It wasn't intended from my side to release this as a 0day exploit. Please complain to security@mozilla.org if you disagree with their release policy.

__Summary

The search plugin technology in Firefox is based on Apple's sherlock files, a simple text format to syndicate a search engine interface. The installer and parser of those files contain design bugs that allow to create a search engine that works as a spyware tool and/or execution vehicle for arbitrary code.

Firesearching 1

By creating a special sherlock file it is possible to run javascript code in the security context of the currently active tab. This allows to create search engines that silently monitor all website displayed while searching (e.g. to steal sessions cookies) and/or that wait for a privileged page (e.g. chrome or about:config) to run arbitrary code.

The demo adds a new search engine (called Firesearching) by calling sidebar.addSearchEngine() that behaves like a normal Google search. When searching with that engine an alert shows that the engine has javascript access to the currently active tab. An attacker could silently send the information to another host instead.

Firesearching 2

By creating a special sherlock file it is possible to overwrite an existing search engine without a chance for the user to see what is going on. The displayed name in the confirmation dialog is given as the third parameter of sidebar.addSearchEngine(), but the displayed name in the search dropdown is

NT-Bugtraq: Firesearching 1 + 2 [Firefox 1.0.2]

taken from the sherlock file. This way it is possible to overwrite the default Google search with a modified version that monitors the data and/or waits for a chance to run code. The string "google.src" in the source URL got also be moved out of the dialog by supplying a really long URL to the sherlock file (the dialog just cuts the source URL when it's getting too long).

The user will probably think the search engine installation just failed, because after confirming the installation dialog Firefox never displays an error messages if the installation failed because e.g. the sherlock file is broken or not found. Since there is no UI to see details about the installed searches a common user will probably never find out that the default Google search got modified. Using the built in sherlock update feature an attacker also gets a decent update mechanism to modify the scripts beyond the initial infection.

__Proof-of-Concept

<http://www.mikx.de/firesearching/>

__Status

The bugs are fixed in Firefox 1.0.3. Don't install search plugins as a workaround.

2005-04-12 Vendor informed (bugzilla.mozilla.org #290037 and #290038)

2005-04-12 Vendor confirmed bug

2005-04-15 Vendor published fix, advisory and link to PoC (mfsa2005-38)

2005-04-18 This advisory

__Affected Software

Tested with Firefox 1.0.2

__Contact Informations

Michael Krax <mikx@mikx.de>

<http://www.mikx.de/?p=14>

mikx

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--