

Re: Mozilla protocol abuse

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-07/msg00302.html>

- *From:* Thor Larholm <seclists@xxxxxxxxxxx>
 - *Date:* Thu, 26 Jul 2007 03:32:15 +0200
-

Since I published this report it has come to my attention that Thunderbird 1.5, unlike Thunderbird 2.0, has not been patched with the "osint" security flag. As such all Thunderbird 1.5 users are vulnerable against this attack and those exploits. Now would be a good time to upgrade to Thunderbird 2.0.

<http://larholm.com/2007/07/26/thunderbird-15-has-not-been-patched-with-osint/>

Regards
Thor Larholm

Thor Larholm wrote:

The Mozilla application platform currently has an unpatched input validation flaw which allows you to specify arbitrary command line arguments to any registered URL protocol handler process. Jesper Johansson already detailed parts of this on his blog on July 20, <http://msinfluentials.com/blogs/jesper/>. I wrote a vulnerability report on July 18 together with a proof-of-concept exploit that targeted Thunderbird 2.0.0.4.

Thunderbird 2.0.0.5 was released on July 19 and incidentally fixed this specific attack vector through its "osint" command line flag. It is now 6 days later and people should have had time to update their Thunderbird installations, so I have decided to publish my vulnerability report together with the exploits as they detail how to handle XPI exploitation.

The HTML version can be found at

<http://larholm.com/2007/07/25/mozilla-protocol-abuse/>

A ZIP file with the report and the XPI exploits can be found at

<http://larholm.com/media/2007/7/mozillaprotocolabuse.zip>

Cheers
Thor Larholm