

Full-Disclosure: [Full-disclosure] FireFox "Host:" Buffer Overflow is not just exploitable on FireFox

[Full-disclosure] FireFox "Host:" Buffer Overflow is not just exploitable on FireFox

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0324.html>

From: Berend-Jan Wever (berendjanwever_at_gmail.com)

Date: 09/11/05

Date: Sun, 11 Sep 2005 01:39:27 -0700

To: full-disclosure@lists.grok.org.uk, bugtraq@securityfocus.com, security@mozilla.org, security@

Hi all,

Research and development has let to a ~90% reliable working exploit for the IDN Heap Buffer overrun in FireFox on WinXP and Win2k3 as long as DEP is turned off and JavaScript is enabled. Some tweaking might yield an even higher success ratio. It has also revealed that not only FireFox is vulnerable to this vulnerability, but the exact same exploit works on the latest releases of all these products based on the Mozilla engine:

- Mozilla FireFox 1.0.6 and 1.5beta,
- Mozilla Browser 1.7.11,
- Netscape 8.0.3.3 <<http://8.0.3.3>>.

Recommendations for this vulnerability:

- FireFox and Mozilla: Install the workaround for (<https://addons.mozilla.org/messages/307259.html>).
- Netscape: hope they'll respond to this email and release a workaround.
- Wait for a patch and install it asap.

Recommendations to make it harder to exploit any FireFox vulnerability:

- Turn on DEP (Data Execution Prevention),
- Turn off JavaScript,
- Switch to another browser,
- Do not browse untrusted sites,
- Do not browse the web at all,
- Unplug your machine from the web,
- Wear a tinfoil hat.

Cheers,

SkyLined

On 9/10/05, Berend-Jan Wever <berendjanwever@gmail.com> wrote:

>

> *(Just a little heads up, no details or PoC attached)*

> *The security vulnerability in Mozilla FireFox reported by Tom Ferris is exploitable on Windows.*

> *I developed a working exploit that seems to be 100% stable, though I've only tested it on one system.*

> *The exploit will not be released publicly until patches are out.*

> *On a side note: it took only about 3 hours and 30 minutes to develop the*

[Full-disclosure] FireFox "Host:" Buffer Overflow is not just exploitable on FireFox

Full-Disclosure: [Full-disclosure] FireFox "Host:" Buffer Overflow is not just exploitable on FireFox

> *exploit, so I might not be the only one able to write it.*
> *Cheers,*
> *SkyLined*
>
> --
> *Berend-Jan Wever <berendjanwever@gmail.com>*
> <http://www.edup.tudelft.nl/~bjwever>
>

--
Berend-Jan Wever <berendjanwever@gmail.com>
<http://www.edup.tudelft.nl/~bjwever>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>