

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

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0400.html>

---

**From:** Juha-Matti Laurio ([juha-matti.laurio\\_at\\_net.fi](mailto:juha-matti.laurio_at_net.fi))

**Date:** 09/13/05

Date: Wed, 14 Sep 2005 00:35:37 +0300 (EEST)

To: [berendjanwever@gmail.com](mailto:berendjanwever@gmail.com)

>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

BTW: From where is that security [at] netscape.org address?

1)

An official security URL to Netscape is "Netscape Browser Bug Submission Form" at

<http://browser.netscape.com/ns8/support/bugreport.jsp>

(www.netscape.org redirects to home.netscape.com/ , of course they have netscape.org, netscape.net etc.)

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

For version 7.2 (and 7.x?) it is the following:

<http://wp.netscape.com/browsers/7/feedback/problem.html>

Two separate addresses due to different developer teams, according to my knowledge. Is there any new information?

I have informed the vendor Netscape being affected on 9th September 2005.

2)

Disabling IDN support via about:config (or prefs.js file) is possible in Netscape Browser 8 too. Xpi file for Firefox and Mozilla Suite works in Netscape 8.0.3.3 too. Test was successful and even UA was changed to include ....Gecko/20050729 (No IDN) Netscape/8.0.3.3.

However, the manual method is recommended.

I.e. there is a workaround for Netscape. Vendor developer team contacted during a weekend, no reply yet.

3)

When an updated version of Netscape Browser 8 is available the download link is <http://browser.netscape.com/ns8/download/default.jsp>

– Juha-Matti

---

Full-Disclosure – We believe in it.

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

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