

[NEWS] Gecko Based Browser IDN Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0052.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/13/05

To: list@securiteam.com

Date: 13 Sep 2005 16:09:02 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Gecko Based Browser IDN Buffer Overflow

SUMMARY

A buffer overflow vulnerability exists within Gecko based web browsers that allows for a remote attacker to execute arbitrary code on a remote host.

DETAILS

Vulnerable Systems:

- * Firefox version 1.0.6 and prior
- * Firefox version 1.5 Beta 1 (Deer Park Alpha 2)
- * Mozilla Suite version 1.7.11 and prior
- * Netscape version 7.x
- * Netscape version 8.x

The problem seems to be when a hostname which has all dashes causes the NormalizeIDN call in nsStandardURL::BuildNormalizedSpec to return true, but is sets encHost to an empty string. Meaning, Firefox appends 0 to approxLen and then appends the long string of dashes to the buffer instead.

Debug information:

(gdb) x/i \$eip

Securiteam: [NEWS] Gecko Based Browser IDN Buffer Overflow

```
0x867926c <_ZN16nsTypedSelection5ClearEP14nsIPresContext+2236>:  
    call *0x4(%eax)  
(gdb) info reg eax  
eax 0x61616161 1633771873
```

Proof of Concept:

Create a link as followed:

< A HREF=https:----- >

Vendor Status:

Mozilla foundation has released a patch for Firefox:

<<http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.6/patches/307259.xpi>>

<http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.6/patches/307259.xpi>

Installing the Patch:

1. In the Software Installation window, click the "Install Now" button.
2. Exit and restart your Mozilla or Firefox browser.
3. To verify the fix in Firefox and the Mozilla Suite, be sure to restart the browser and then follow these steps:
 4. In Firefox Click Help -> About Mozilla Firefox and verify that the user agent string contains "(noIDN)"
 5. In the Mozilla Suite Click Help -> About Mozilla and verify that the user agent string contains "(noIDN)"

Manually Configuring the Browser:

To manually change the browser configuration for Firefox or the Mozilla Suite, follow these instructions:

1. Type about:config into the address field and hit Enter.
2. In the Filter toolbar, type network.enableIDN.
3. Right click on the the network.enableIDN item and select toggle to change value to false.

To verify the fix in your Firefox or Mozilla application, be sure to restart the browser and then follow these steps.

1. Type about:config into the address field and hit Enter.
2. In the Filter toolbar, type network.enableIDN.
3. Ensure that the the value for this item is set to false.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2871>>
CAN-2005-2871

Disclosure Timeline:

September 4, 2005 Reported

September 4, 2005 Public Released

ADDITIONAL INFORMATION

The information has been provided by <mailto:juha-matti.laurio@netti.fi>

Juha-Matti Laurio,

<mailto:venglin@freebsd.lublin.pl> Przemyslaw Frasunek

Securiteam: [NEWS] Gecko Based Browser IDN Buffer Overflow

The vendor advisory can be found at:

<<https://addons.mozilla.org/messages/307259.html>>

<https://addons.mozilla.org/messages/307259.html>

The vendor bug report can be found at:

<https://bugzilla.mozilla.org/show_bug.cgi?id=307259>

https://bugzilla.mozilla.org/show_bug.cgi?id=307259

The CERT advisory can be found at:

<<http://www.kb.cert.org/vuls/id/573857>>

<http://www.kb.cert.org/vuls/id/573857>

The original advisory can be found at:

<<http://security-protocols.com/advisory/sp-x17-advisory.txt>>

<http://security-protocols.com/advisory/sp-x17-advisory.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.