

[NEWS] Gecko based browsers Stack Corruption

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/26/05

To: list@securiteam.com

Date: 26 Sep 2005 12:52:11 +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 browsers Stack Corruption

SUMMARY

Lack of proper length and value checking allow attacker to cause a buffer overflow and execute arbitrary code or cause a DoS using Gecko based web browsers.

DETAILS

Vulnerable Systems:

- * Mozilla firefox 1.0.6 and prior
- * Netscape Browser version 8.0.3.3
- * K-Meleon Browser version 0.9

Immune Systems:

- * Mozilla firefox 1.0.7

Stack Corruption:

The problem existed in "zero-width non-joiner" sequence of unicode chars that uses Arabic shaping style. Because the code did not checked for buffer length before manipulating the given text. On a crafted content, it is possible to cause the buffer to be twice the size the actual data, and memory allocated for the buffer itself.

Securiteam: [NEWS] Gecko based browsers Stack Corruption

Proof of Concept:

```
< html>
< body>
& #8204;& #8204;& # 8204;& #8204;& #8204;& #8204;& #8204;& #8204;& #1742;
& #8204;& #8204;& #1740;& #8204;
< /body>
< /html>
```

CVE Information:

```
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2702>
CAN-2005-2702
```

ADDITIONAL INFORMATION

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

The original article can be found at:

```
<http://www.mozilla.org/security/announce/mfsa2005-58.html>
```

```
http://www.mozilla.org/security/announce/mfsa2005-58.html
```

The bug report can be found at:

```
<https://bugzilla.mozilla.org/show\_bug.cgi?id=296134>
```

```
https://bugzilla.mozilla.org/show\_bug.cgi?id=296134
```

=====

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.