

[NEWS] Mozilla Firefox SVG Processing Remote Code Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00040.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 16:48:58 +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>

Mozilla Firefox SVG Processing Remote Code Execution Vulnerability

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Mozilla Firefox. User interaction is required to exploit this vulnerability in that the target must visit a malicious page.

DETAILS

The specific flaw exists in the browser's handling of SVG comment objects. Firefox does not correctly handle requests to append SVG comments to elements in other types of documents. Attempting such an operation results in a memory corruption that can be exploited to execute arbitrary code.

Vendor Response:

Mozilla has issued an update to correct this vulnerability. More details can be found at:

<<http://www.mozilla.org/security/announce/2006/mfsa2006-73.html>>
<http://www.mozilla.org/security/announce/2006/mfsa2006-73.html>

CVE Information:

[NEWS] Mozilla Firefox SVG Processing Remote Code Execution Vulnerability

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6504>>
CVE-2006-6504

Disclosure Timeline:

2006.11.08 – Vulnerability reported to vendor
2006.12.12 – Digital Vaccine released to TippingPoint customers
2006.12.19 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
Zero Day Initiative.

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-06-051.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-06-051.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.