

[NEWS] Sun Microsystems Java GIF File Parsing Memory Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-01/msg00046.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 17 Jan 2007 17:26:57 +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>

Sun Microsystems Java GIF File Parsing Memory Corruption Vulnerability

SUMMARY

This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Sun Microsystems Java Virtual Machine (JVM). User interaction is required to exploit this vulnerability in that the target must visit a malicious website.

DETAILS

Affected Products:

- * JDK and JRE version 5.0 Update 9 and earlier (all platforms)
- * SDK and JRE version 1.4.2_12 and earlier (all platforms)
- * SDK and JRE version 1.3.1_18 and earlier (all platforms)

The specific flaw exists during the parsing of GIF image components. When the image width in an image block of a valid GIF file is set to 0, the Java runtime will allocate the specified size but subsequently copy all data to the under allocated memory chunk. The overflow results in the corruption of multiple pointers, at least one of which is later dereferenced and can therefore result in execution of arbitrary code.

[NEWS] Sun Microsystems Java GIF File Parsing Memory Corruption Vulnerability

Vendor Response:

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

<<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-102760-1>>
<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-102760-1>

Disclosure Timeline:

- 2006.06.16 – Vulnerability reported to vendor
- 2006.12.18 – Digital Vaccine released to TippingPoint customers
- 2007.01.16 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0243>>
CVE-2007-0243

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-07-005.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-005.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.