

[NEWS] Adobe Flash Player JPG Processing Heap Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00053.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2007 16:34:09 +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>

Adobe Flash Player JPG Processing Heap Overflow Vulnerability

SUMMARY

A vulnerability allows remote attackers to execute arbitrary code on systems with vulnerable installations of the Adobe Flash Player. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

DETAILS

The specific flaw exists in the Flash Player's parsing of JPG images embedded in SWF files. The Flash Player trusts the signed X and Y densities specified in the JPG header and makes memory allocations accordingly. A processing loop later treats these values as unsigned, leading to excessive loop iterations and heap corruption while decoding the rest of the image.

Vendor Response:

Adobe has released patches, details can be found at:

<<http://www.adobe.com/support/security/bulletins/apsb07-20.html>>

<http://www.adobe.com/support/security/bulletins/apsb07-20.html>

[NEWS] Adobe Flash Player JPG Processing Heap Overflow Vulnerability

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6242>>
CVE-2007-6242

Disclosure Timeline:

2007.11.02 – Vulnerability reported to vendor
2007.12.19 – Coordinated public release of advisory

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tsrt@xxxxxxxx>> TippingPoint
DVLabs.

The original article can be found at:

<<http://dvlabs.tippingpoint.com/advisory/TPTI-07-21>>
<http://dvlabs.tippingpoint.com/advisory/TPTI-07-21>

=====

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.