

[NEWS] Opera Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-06/msg00021.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 11 Jun 2006 15:06:19 +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>

Opera Buffer Overflow

SUMMARY

" <<http://www.opera.com/>> Opera is the most full-featured Internet power tool on the market, Opera includes pop-up blocking, tabbed browsing, integrated searches, and advanced functions like Opera's groundbreaking E-mail program, RSS Newsfeeds and IRC chat."

Improper input validation allows attackers to execute arbitrary code using a buffer overflow in Opera.

DETAILS

Vulnerable Systems:

- * opera version 8.53 and prior

Immune Systems:

- * opera version 8.54

A buffer overflow in the code processing style sheet attributes was found. It is caused by an integer signedness error in a length check followed by a call to a string function. It seems to be hard to exploit this buffer overflow to execute arbitrary code because of the very large amount memory

[NEWS] Opera Buffer Overflow

that has to be copied.

A remote attacker can entice a user to visit a web page containing a specially crafted style sheet attribute that will crash the user's browser and maybe lead to the execution of arbitrary code.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1834>>
CVE-2006-1834

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jaervosz@xxxxxxxxxx>> Sune Kloppenborg Jeppesen.

The original article can be found at:

<<http://www.gentoo.org/security/en/glsa/glsa-200606-01.xml>>
<http://www.gentoo.org/security/en/glsa/glsa-200606-01.xml>

=====

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.