

[NEWS] Firefox and Opera Memory Information Leak

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00068.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 17 Feb 2008 08:31:32 +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>

Firefox and Opera Memory Information Leak

SUMMARY

Opera and Firefox contains vulnerable code for handling BMP files with partial palette. The code allows to craft a BMP file that leaks information from the heap. This information can be sent to remote server using canvas tag (HTML 5) and JavaScript.

Also other browser (for example Apple Safari) contain vulnerable BMP handling code, but since there is no way of acquiring the image data (due to not all canvas method being implemented), it doesn't pose a serious threat. As a matter of fact Apple Safari has a similar problem with certain GIF files.

DETAILS

Vulnerable Systems:

- * Firefox version 2.0.0.11 and prior that support `canvas.getImageData` or any other method to acquire image data are affected
- * Opera version 9.50 beta

Immune Systems:

[NEWS] Firefox and Opera Memory Information Leak

- * Firefox version 2.0.0.12
- * Opera version 9.24
- * Opera version 9.25

The BMP format has a field in the BITMAPINFOHEADER named biClrUsed, the field says how many colors does the palette contain. If this field is 0, then 256 color palette is used. When this field is not 0, the palette has the given number of colors.

Both browsers either allocate to just the "right" amount of memory (using the equation $biClrUsed * sizeof(RGB)$), or forget to zero the allocated palette. In this case, if a color from the upper (non existing or not zeroed) part of the palette is used, some information is copied to the screen as a colorful pixel.

If the attacker creates a BMP file with biClrUser = 0, and fills it with gradient, from 0 to 255: 00 01 02 03 04 05 ... and so on, the displayed BMP will in fact copy the palette to the screen, which of course means that it copies the data lying on the heap to the screen.

The attacker could also use HTML 5 tag canvas to acquire pixel color information from the bitmap, and then use JavaScript to post it to a remote server.

The harvested data contains various information including parts of other websites, users "favorites" and history, and other information.

Additional info:

Firefox 2.0.0.11 may crash when using this vulnerability due to heap boundary error (read access violation). So it is possible to remotely crash the browser.

Video demonstration

A video demonstration of the vulnerability can be found on the following sites:

<<http://blog.hispasec.com/lab/>> <http://blog.hispasec.com/lab/>
<<http://vexillium.org/?sec=ff>> <http://vexillium.org/?sec=ff>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:gynvael@xxxxxxxxxxxxxx>>
Gynvael Coldwind.

The original article can be found at: <<http://gynvael.coldwind/vx>>
<http://gynvael.coldwind/vx>

=====

[NEWS] Firefox and Opera Memory Information Leak

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.