

[NT] Opera Arbitrary File Delete Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/24/03

To: list@securiteam.com

Date: 24 Dec 2003 12:26:31 +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 Arbitrary File Delete Vulnerability

SUMMARY

<<http://www.opera.com/>> Opera for "windows is a GUI base web browser".

While Opera displays the Download dialog, it creates a temporary file.

This file name is not sanitized thoroughly, as such, it allows an existing file to be deleted (and overwritten).

DETAILS

Vulnerable systems:

* Opera version 7.22 build 3221 (JP:build 3222)

* Opera version 7.21 build 3218 (JP:build 3219)

* Opera version 7.20 build 3144 (JP:build 3145)

* Opera version 7.1x

* Opera version 7.0x

Immune systems:

* Opera version 7.23 build 3227 (JP:build 3226)

Technical details:

While Opera displays the Download dialog, it will create a temporary file that is based on the name used while downloading the file. This temporary file is used for searching for an associated application.

Securiteam: [NT] Opera Arbitrary File Delete Vulnerability

ex.

Download URL:

"http://server/path/FILENAME.ext"

Temporary Filename:

"c:\windows\temp\FILXXX.tmp.FILENAME.ext"

(XXX is random string, like "01A")

However, this temporary file name is not sanitized thoroughly making it possible to insert illegal characters (for example: '..%5C'). The file with such illegal characters can be placed in any path on the same drive as a temporary directory. If there is already such a file, it will be overwritten and deleted soon.

ex.

Download URL:

"http://server/path/AAAAAAAAAA%5C..%5C..%5Ccalc.exe"

Temporary Filename:

"c:\windows\temp\AAAXXX.tmp.AAAAAAAAAA\..\calc.exe"

this is... "c:\windows\calc.exe"

Therefore, if a user goes to a malicious site that makes Opera display the Download dialog, his files could be deleted using this vulnerability.

The conditions that allow deleting of files:

1. File's path can be specified with a relative path from the Opera's temporary directory
2. File name must contain '.'
3. The file must be writable within Opera process's privileges
4. No "Read Only" attribute under Windows 9x. No "Read Only", "System" or "Hide" attributes under Windows NT/2000

Vendor status:

- * 2003-10-09 Discovered this vulnerability
- * 2003-11-26 Reported to vendor
- * 2003-12-12 Published this advisory

Solution:

Upgrade to version 7.23 or later version.

ADDITIONAL INFORMATION

The original advisory can be found at:

<<http://opera.rainyblue.org/modules/cjaycontent/index.php?id=16>>
<http://opera.rainyblue.org/modules/cjaycontent/index.php?id=16>.

The information has been provided by <mailto:imagine20xx@gmx.net> imagine and <mailto:nesumin@softhome.net> nesumin.

Securiteam: [NT] Opera Arbitrary File Delete Vulnerability

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.