

# [NT] Opera Web Browser Directory Traversal in Internal URI Protocol

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0082.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 11/19/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 19 Nov 2003 19:34:37 +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 Web Browser Directory Traversal in Internal URI Protocol

---

## SUMMARY

Opera Web Browser defines an internal URI Protocol like command called "opera:". Among other things, it is used to display documentation and help files for the browser. It has an input validation flaw that enables directory traversal.

This flaw is an aggravating factor when combined with other vulnerabilities. In this case, it can be combined with the "Opera Skinned" vulnerability.

## DETAILS

Vulnerable systems:

- \* Opera version 7.21 and prior

Immune systems:

- \* Opera version 7.22

NOTE: It is assumed that Opera is installed in the default location i.e., "c:\program files\opera7" for the purpose of this description. However, a

## Securiteam: [NT] Opera Web Browser Directory Traversal in Internal URI Protocol

default install is \*not\* necessary for exploitation.

"Opera:" is an internal URI protocol-like command used by Opera. "Internal" because it is not registered as a URI protocol in the Windows Registry. One of its uses is to display documentation. For instance, to see help, "opera:/help/" is used. This points to the "C:\Program Files\Opera7\help" directory on the file system. The html files in this folder can be accessed through this relative URL, like, "opera:/help/foo.html". When a local path is requested through "opera:" in the form of a legal "opera:/help/" URL, it uses the service of the "file://" protocol. For instance, "opera:/help/" redirects the browser to "file://localhost/C:/Program Files/Opera7/Help/index.html".

"opera:history", "opera:plugins", "opera:cache" and "opera:drives" are other known uses for this command. Their function is self-explanatory. "about:" is an alias for "opera:". For instance, "about:history" translates to "opera:history".

The problem here is that though, using "../" for directory traversal in the opera: command is not allowed and Opera responds with an "illegal address" prompt, this can easily be bypassed using "..%5c" or "..%2f" to break out of the /help/ directory.

For instance, using "opera:/help/..%5c..%5c..%5cwinnt/notepad.exe" downloads "notepad.exe" from the "winnt" folder.

### Exploit:

Exploits that depend on knowing the installation path of Opera are helped by this vulnerability. The command "opera:/help/" always points to the "<opera directory>/help/" directory. This can be used as a reference point for exploits because of the directory traversal. For instance, "opera:/help/..%5c" points to the Opera Directory.

The exploit attached with the advisories uses this vulnerability for getting the correct path of the "<opera dir>/profile/" folder for exploitation.

### Vendor response:

The vendor, Opera Software, deserves special mention here. S G Masood has previously read about Opera Soft's promptness in resolving security vulnerabilities in their products. S G Masood's experience with them is one of the best S G Masood ever had with any vendor. S G Masood hopes they continue to maintain their good record even with future security issues.

An updated version with a fix(7.22) is available from the site – <http://www.opera.com/download/>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:sgmasood@yahoo.com> S G Masood.

Securiteam: [NT] Opera Web Browser Directory Traversal in Internal URI Protocol

=====

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](mailto:list-unsubscribe@securiteam.com)

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