



CYBSEC S.A.

www.cybsec.com

Advisory Name: Denial of Service in WebSphere Edge Server.

Vulnerability Class: Denial of Service

Release Date:

Affected Applications:

- WebSphere Edge Components Caching Proxy 5.02 using JunctionRewrite with UseCookieDirective.

Not Affected Applications:

- WebSphere Edge Components Caching Proxy 5.02 NOT using JunctionRewrite with UseCookie directive.
- WebSphere Edge Components Caching Proxy 5.00

Affected Platforms:

- SUSE SLES 8
- SUSE SLES 8 Service Pack 1
- SUSE SLES 8 Service Pack 3
- SUSE SLES 8 Service Pack 3
- Apparently all platforms running WebSphere Edge Server

Local / Remote: Remote

Severity: High

Author: Leandro Meiners.

Vendor Status:

- Included in WebSphere Application Server 5.0.3 fix (to be released)
- Patch available from IBM for clients with Support Level 2 or 3

Reference to Vulnerability Disclosure Policy:

http://www.cybsec.com/vulnerability_policy.pdf

Overview:

WebSphere Edge Component Caching Proxy, part of WebSphere Application Server, is a reverse proxy designed to reduce bandwidth use and improve a Web site's speed and reliability by providing a point-of-presence node for one or more back-end content servers. It is built to work with content provided by one or more backend WebSphere Application Servers.

Vulnerability Description:

The vulnerability discovered allows a remote attacker to generate a denial of service condition against the WebSphere Edge Component Caching Proxy.

If the reverse proxy is configured with the JunctionRewrite directive being active, a remote attacker can trivially cause a denial of service by executing the GET HTTP method without parameters.

Exploit:

```
$ echo "GET" | nc <victim_host_ip> <proxy_port>
```

Solutions:

If JunctionRewrite is unnecessary, disabling it will suffice to prevent the Denial of Service. Also if the option UseCookie in the JunctionRewrite directive is unnecessary disabling it will suffice to prevent the Denial of Service.

Vendor Response:

IBM opened a case regarding the vulnerability and provided a patch within 2 weeks of the initial contact.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at Imeiners@cybsec.com.

For more information regarding CYBSEC: www.cybsec.com