

[NT] Bea WebLogic Incorrect URL Parsing Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0121.html>

From: support@securiteam.com

Date: 04/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 30 Apr 2002 21:53:13 +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.

Bea WebLogic Incorrect URL Parsing Issues

SUMMARY

The <<http://www.bea.com>> Bea WebLogic server incorrectly parses certain types of URL requests. This can result in the physical path being revealed, a Denial of Service situation, and revealing of .jsp source code.

DETAILS

Vulnerable systems:

- Bea WebLogic version 6.1 Service Pack 2 on Windows 2000 Server

A problem with the URL parser in Bea WebLogic could allow a malicious user to reveal the physical path to the web root, cause a Denial of Service, and reveal the source code of .jsp files.

Physical web root:

By appending %00.jsp to a normal .html request, a compiler error would in some cases be generated that would print out the path to the physical web root. A similar result can be achieved by prefixing with %5c (backslash).

Denial of Service:

This issue is very similar to the one reported in KPMG-2002003, in which we published that requesting a DOS device and appending .jsp to the

Securiteam: [NT] Bea WebLogic Incorrect URL Parsing Issues

request would exhaust the working threads and cause the web service to stop parsing HTTP and HTTPS requests.

If a malicious user also added %00 in the request, it would still work.

The server can handle about 10–11 working threads, so when this number of active threads has been reached, the server will no longer service any requests. Since both HTTP and HTTPS are handled by the same module, both are crippled if one is attacked.

Source code revealed:

There are a number of ways to manipulate the URL in a way that will allow a malicious user to read the contents of a .jsp file. One way is to append "%00x" to the request, another could be to add "+" to the request (exclamation marks excluded).

Vendor response:

The vendor was contacted about the first issue on the 6th of November, 2001 and subsequently on the 12th of March, 2002 and finally on the 22nd of March, 2002 about the remaining issues. On the 25th of March, 2002 we received a private hotfix, which corrected the issues. On the 22nd of April, 2002 the vendor released a public bulletin.

The vendor's bulletin can be seen here: (note that the URL has been wrapped for readability)

<http://dev2dev.bea.com/resourcelibrary/advisoriesdetail.jsp?highlight=advisoriesnotificationsdev2dev/resourcelibraryhttp://dev2dev.bea.com/resourcelibrary/advisoriesdetail.jsp?highlight=advisoriesnotifications&path=components/dev2dev/resourcelibrary/advisoriesnotifications/securityadvisoriesbea020303.htm>

Be sure you read the vendor bulletin, as it suggests other security settings that might prevent future similar issues.

Corrective action:

The following has been copied from the vendor bulletin:

"BEA WebLogic Server and Express version 6.1 standalone or as part of BEA WebLogic Enterprise 6.1 on all OS platforms Action: Apply Service Pack 2 and then apply this patch:

ftp://ftpna.bea.com/pub/releases/security/CR069809_610sp2_v2.jar

When Service Pack 3 becomes available, you can use that jar instead of Service Pack 2 and this patch.

BEA WebLogic Server and Express version 6.0 standalone or as part of BEA WebLogic Enterprise 6.0 on all OS platforms Action: Apply Service Pack 2 with Rolling Patch 3 and then apply this patch:

ftp://ftpna.bea.com/pub/releases/security/CR069809_60sp2rp3.jar

Securiteam: [NT] Bea WebLogic Incorrect URL Parsing Issues

ftp://ftpna.bea.com/pub/releases/security/CR069809_60sp2rp3.jar

BEA WebLogic Server and Express version 5.1 standalone or as part of BEA WebLogic Enterprise 5.1.x on all OS platforms Action: Apply Service Pack 11 and then apply this patch:

<ftp://ftpna.bea.com/pub/releases/security/CR069809_510sp11_v2.jar>

ftp://ftpna.bea.com/pub/releases/security/CR069809_510sp11_v2.jar

When Service Pack 12 becomes available, you can use that jar instead of Service Pack 11 and this patch.

BEA WebLogic Server and Express 4.5.2 on all OS platforms Action: Apply Service Pack 2 and then apply this patch:

<ftp://ftpna.bea.com/pub/releases/security/CR045420_wls452sp2.zip>

ftp://ftpna.bea.com/pub/releases/security/CR045420_wls452sp2.zip

BEA WebLogic Server and Express 4.5.1 on all OS platforms Action: Apply Service Pack 15."

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pgrundl@kpmg.dk>> Peter Gründl.

=====

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: "[NT] Method Found to Bypass ATGuard's Firewall"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)