

[NT] BEA WebLogic Performance Pack Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0022.html>

From: support@securiteam.com

Date: 07/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 8 Jul 2002 23:44:44 +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 Performance Pack Denial of Service

SUMMARY

If the performance pack is enabled, the BEA WebLogic Server can be crashed by a malicious user. The performance pack is enabled in a default installation.

DETAILS

Vulnerable systems:

– BEA WebLogic 7.0 on Windows 2000 Server

* BEA WebLogic Server and Express 5.1.x, 6.0.x, and 6.1.x on Microsoft NT or Windows 2000.

<<http://www.bea.com/>> BEA WebLogic was designed for enterprise applications that demand the flexibility and security of server-side components in Java, BEA WebLogic server brings scalability, performance, and fault tolerance to mission-critical Web-based solutions. BEA WebLogic Server is an award-winning Java application server for developing, deploying, and managing Web applications. BEA WebLogic Server also offers the most complete implementation of the Java 2 Enterprise Edition standard – including Enterprise JavaBeans.

Securiteam: [NT] BEA WebLogic Performance Pack Denial of Service

The Bea WebLogic Server is vulnerable to a data/connection flooding that will result in the web service crashing with a report of an error in NTDLL.DLL.

Vendor response:

The vendor was notified on 1 May 2002. On 2 May 2002, the vendor had reproduced the issue and assigned case number 324070 and change request CR076409 to the issue. On 17 May 2002, the vendor supplied us with a workaround for the issue. On 3 July, the vendor issued an official patch for the issue.

Corrective action:

As a temporary workaround, you can disable the performance pack:

1. Start the WebLogic Server Console.
2. Open the Servers folder in the navigation tree.
3. Select your server in the Servers folder.
4. Select the Configuration tab.
5. Select the Tuning tab.
6. If the "Native IO Enabled" check box is selected, uncheck it.
7. Click Apply.
8. Restart your server.

The vendor released bulletin, containing links to the official patches, can be accessed through this URL (wrapped for readability):

<http://dev2dev.bea.com/resourcelibrary/advisoriesdetail.jsp?highlight=advisoriesnotificationsdev2dev/resourcelibrary/http://dev2dev.bea.com/resourcelibrary/advisoriesdetail.jsp?highlight=advisoriesnotificationsdev2dev/resourcelibrary/>

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.

Securiteam: [NT] BEA WebLogic Performance Pack Denial of Service

- **Previous message:** support@securiteam.com: "[TOOL] IE'en Remotely Controls Internet Explorer using DCOM"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)