

[NT] Bea Weblogic DOS device Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0061.html>

From: support@securiteam.com

Date: 01/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 14 Jan 2002 14:45:59 +0100 (CET)

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 DOS device Denial of Service

SUMMARY

A flaw in the way the <<http://www.beasys.com>> Bea Weblogic server handles specific requests containing DOS-devices can cause a Denial of Service condition, where web requests are no longer being serviced.

DETAILS

Vulnerable systems:

Bea Weblogic Server 6.1 Service Pack 1 for Windows NT/2000

When the Weblogic server receives a .jsp request, it invokes an external compiler to deal with the .jsp resource requested. The server can be fooled into thinking you are requesting a valid .jsp resource by simply requesting a DOS-device (such as 'aux' for example) and appending the .jsp extension to it (aux.jsp). The external compiler is then invoked and due to the nature of the DOS-devices, this working thread never finishes.

The server can handle about a 10-11 working threads, so when this number of active threads is 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.

Securiteam: [NT] Bea Weblogic DOS device Denial of Service

Vendor response:

The vendor was contacted on the 6th of November, 2001. On the 15th of November the vendor confirmed that they have reproduced the issue on Windows 2000 and Windows NT. The issue is assigned the bug id: CR062542 by the vendor. On the 3rd of January, 2002 the vendor confirmed the release of the new service pack and that it included the patch for this issue.

Corrective action:

Upgrade to Service Pack 2, which can be downloaded here:
<<http://commerce.beasys.com>> <http://commerce.beasys.com>

ADDITIONAL INFORMATION

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

=====

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: "[NEWS] User Posting Vulnerability in Nick.com Forums (Nickelodeon)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)