

[NEWS] Multiple Vulnerabilities in BEA WebLogic Server (Un-authenticated File Uploading)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0050.html>

From: support@securiteam.com

Date: 03/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 18 Mar 2003 17:08:22 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Multiple Vulnerabilities in BEA WebLogic Server (Un-authenticated File Uploading)

SUMMARY

WebLogic offers a web management console through which you can manage the web server contents, load servlets, etc. One of the functionalities it offers is that you can upload files to the remote server for its publication.

The process in charge of managing the file upload validates the user credentials and then calls an internal WebLogic servlet to upload the file that does not require any authentication. This internal servlet can be publicly accessed and therefore it is possible to upload files to the server without any kind of authentication.

DETAILS

Affected Versions and platforms:

These vulnerabilities have been verified to work in the WebLogic version for Windows and Linux, although we think that they are not specific to the

platform.

The current vulnerabilities vary in the different versions, the following table shows which vulnerabilities are present in each version:

UPLOAD DOWNLOAD PASSWORD

WebLogic 6.0 X X
WebLogic 6.1 X X X
WebLogic 7.0 X

The WebLogic Server 5.1 version does not present any of the previously mentioned vulnerabilities.

Technical details:

Files can be uploaded to any location in the remote server, not limiting to the tree of WebLogic directories (in Windows 2000 it is possible to upload files to any disk drive).

If you know the directory where the WebLogic server applications have been installed (such as in a default installation) there is the possibility to upload a malicious application that will allow an attacker to execute commands with the permissions of the user executing the WebLogic server.

Additionally, the internal servlet offers different operations that allow, without any authentication:

- * Download arbitrary files from the remote server
- * Obtain the users, groups and passwords (salted and hashed) of WebLogic

Solution:

The vendor was notified and published a patch to solve these vulnerabilities. More information on how to get and install the patch can be found in BEA's security advisory

<<http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03-28.jsp>> BEA03-28.00.

If upgrading is not an option, there is a temporary workaround for the problem that consists in the installation of a ConnectionFilter class to filter out requests to the administration server, avoiding exploitation of the vulnerability from the outside world.

In order to apply this workaround the administration and application servers must be running on separate ports. Once they are separated, the ConnectionFilter will filter connections based on the request source address.

S21SEC developed a ConnectionFilter class that allows filtering based on the source address and destination port. This filter along with detailed instructions on how to install and configure the filter can be downloaded from:

Securiteam: [NEWS] Multiple Vulnerabilities in BEA WebLogic Server (Un-authenticated File Uploading)

<<http://www.s21sec.com/download/s21sec-weblogic-connectionfilter-1.0.tar.gz>>
<http://www.s21sec.com/download/s21sec-weblogic-connectionfilter-1.0.tar.gz>

Alternatively, connections to the administrative server can be filtered by using an IP filtering device.

ADDITIONAL INFORMATION

The original advisory can be downloaded by going to:
<<http://www.s21sec.com/en/avisos/s21sec-011-en.txt>>
<http://www.s21sec.com/en/avisos/s21sec-011-en.txt>

The information has been provided by <<mailto:llmora@s21sec.com>> Lluís Mora.

=====

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.