

[VulnWatch] [AppSecInc Advisory BEA05-V0100] BEA WebLogic Administration Console error page cross-site scripting vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-05/0024.html>

From: Team SHATTER (*shatter_at_appsecinc.com*)

Date: 05/27/05

Date: Fri, 27 May 2005 14:26:26 -0400

To: bugtraq@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

BEA WebLogic Administration Console error page cross-site scripting
vulnerability

AppSecInc Team SHATTER Security Advisory BEA05-V0100
<http://www.appsecinc.com/resources/alerts/general/BEA-001.html>
May 27, 2005

Affected versions: BEA WebLogic Server 7.0 and 8.1

Risk level: High

Credits: This vulnerability was discovered and researched by Agustín
Martínez Fayó of Argeniss for Application Security Inc.

Background:

The Administration Console is a web browser-based, graphical user
interface used to manage a WebLogic Server domain. The Administration
Console supports a full range of product administrative tasks. A
cross-site scripting vulnerability exists in the login page of the
Console.

Details:

Cross-site scripting vulnerabilities occur when an attacker tricks a
legitimate web application into sending malicious code, generally in
the form of a script, to an unsuspecting end user. The attack usually
involves crafting a hyperlink with malicious script code embedded
within it. A valid user is likely to click on this link since it
points to a resource on a trusted domain. The link can be posted on a
web page, or sent in an instant message, or email. Clicking the link
executes the attacker-injected code in the context of the trusted web

application. Typically, the code steals session cookies, which can then be used to impersonate a valid user.

Parameters provided to the error page of the Administration Console are vulnerable to cross-site scripting attacks. User-supplied input to these parameters is returned without proper sanitization, allowing a malicious attacker to inject arbitrary scripting code.

To get the session cookie a remote attacker could send this link to the administrator:

[http://vulnerable.site:7001/console/a?=>alert\(document.cookie\)</script>](http://vulnerable.site:7001/console/a?=>alert(document.cookie)</script>)

Impact:

Attackers can steal administrator's session cookies and password, thereby allowing the attacker to impersonate the valid user.

Workaround:

There is no workaround for this issue.

Vendor Status:

Vendor was contacted and a patch was released.

Fix:

For BEA WebLogic Server and WebLogic Express 8.1 upgrade to Service Pack 4. Apply the patch on top of it located at ftp://ftpna.bea.com/pub/releases/security/CR202495_810sp4.jar on top of the service packs.

For BEA WebLogic Server and WebLogic Express 7.0 upgrade to Service Pack 6. Apply the patch located at ftp://ftpna.bea.com/pub/releases/security/CR214457_700sp6.jar on top of the service packs.

Links:

Application Security, Inc advisory:

<http://www.appsecinc.com/resources/alerts/general/BEA-001.html>

BEA Advisory: <http://dev2dev.bea.com/pub/advisory/130>

— — —

Application Security, Inc.

www.appsecinc.com

AppSecInc is the leading provider of database security solutions for the enterprise. AppSecInc products proactively secure enterprise applications at more than 300 organizations around the world by discovering, assessing, and protecting the database against rapidly changing security threats. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business.

ch: [VulnWatch] [AppSecInc Advisory BEA05-V0100] BEA WebLogic Administration Console error page cross-site scripti

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.0 (MingW32)

iD8DBQFC12ZS/0w1dSVRt4URAJbbAJ9sjbn1lxaldQGxjVgceKakOspAkQCgq+Ur

MyVIFkq5xzvNLsoO3F36C5k=

=+vls

-----END PGP SIGNATURE-----