

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [bugtraq](#)
Subject: [\[security bulletin\] HPSBMU02736 SSRT100699 rev.1 - HP Business Availability Center \(BAC\) a](#)
From: [security-alert\(.\)hp ! com](#)
Date: [2012-01-18 22:46:28](#)
Message-ID: [20120118224628.DB21820591\(.\)security ! hp ! com](#)
[Download RAW [message](#) or [body](#)]

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

Hash: SHA1

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c03127140
Version: 1

HPSBMU02736 SSRT100699 rev.1 - HP Business Availability Center (BAC) and Business \
Service Management (BSM), Remote Unauthorized Access to Sensitive Information

NOTICE: The information in this Security Bulletin should be acted upon as soon as \
possible.

Release Date: 2011-12-18
Last Updated: 2012-01-18

Potential Security Impact: Remote unauthorized access to sensitive information

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified with HP Business Availability \
Center (BAC) and Business Service Management (BSM) . The vulnerabilities could be \
remotely exploited to allow unauthorized access to sensitive information.

References: CVE-2010-1428, CVE-2010-1429, CVE-2008-3273

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
Business Availability Center (BAC) v8.07 and earlier on Windows and Solaris
Business Service Management (BSM) v9.12 and earlier on Windows

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2010-1428	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2010-1429	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2008-3273	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0

Information on CVSS is documented
in HP Customer Notice: HPSN-2008-002

RESOLUTION

HP has made the following procedures available to resolve the vulnerabilities.

For Windows

Disable JBoss WebConsole

Rename:

\HPBAC\EJBContainer\server\mercury\deploy\jmx-console.war
\HPBAC\EJBContainer\server\mercury\deploy\management\console-mgr.sar\web-console.war

To:
\HPBAC\EJBContainer\server\mercury\deploy\jmx-console.war.disable
\HPBAC\EJBContainer\server\mercury\deploy\management\console-mgr.sar\web-console.war.disable

Note: The JBoss WebConsole is disabled in BSM v9.10 and subsequent. The changes above \
are only needed for versions prior to v9.10.

Disable Status Servlet

Edit this file

BAC 8.7: \HPBAC\EJBContainer\server\mercury\deploy\jbossweb-tomcat55.sar\ROOT.war\WEB-INF\web.xml
BSM 9.x: \HPBSM\EJBContainer\server\mercury\deploy\jboss-web.deployer\ROOT.war\WEB-INF\web.xml
to add <!-- and --> as follows:

<!--

```
<servlet>
<servlet-name>Status Servlet</servlet-name>
<servlet-class>org.jboss.web.tomcat.tc5.StatusServlet</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>Status Servlet</servlet-name>
<url-pattern>/status</url-pattern>
</servlet-mapping>
```

- -->

For Solaris

For Solaris the procedure is the same as for Windows.

The Solaris files are:

```
/opt/HPBAC/EJBContainer/server/mercury/deploy/mx-console.war
/opt/HPBAC/EJBContainer/server/mercury/deploy/management/console-mgr.sar/web-console.war
BAC 8.7: /opt/HPBAC/EJBContainer/server/mercury/deploy/jbossweb-tomcat55.sar/ROOT.war/WEB-INF/web.xml
BSM 9.x: /opt/HPBSM/EJBContainer/server/mercury/deploy/jboss-web.deployer/ROOT.war/WEB-INF/web.xml
```

HISTORY

Version:1 (rev.1) 18 January 2012 Initial release

Third Party Security Patches: Third party security patches that are to be installed \ on systems running HP software products should be applied in accordance with the \ customer's patch management policy.

Support: For issues about implementing the recommendations of this Security Bulletin, \ contact normal HP Services support channel. For other issues about the content of \ this Security Bulletin, send e-mail to security-alert@hp.com.

Report: To report a potential security vulnerability with any HP supported product, \ send Email to: security-alert@hp.com

Subscribe: To initiate a subscription to receive future HP Security Bulletin alerts \ via Email: http://h41183.www4.hp.com/signup_alerts.php?jumpid=hpsec_bulletins

Security Bulletin List: A list of HP Security Bulletins, updated periodically, is \ contained in HP Security Notice HPSN-2011-001: \ https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c02964430

Security Bulletin Archive: A list of recently released Security Bulletins is \ available here: <http://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive/>

Software Product Category: The Software Product Category is represented in the title \ by the two characters following HPSB.

```
3C = 3COM
3P = 3rd Party Software
GN = HP General Software
HF = HP Hardware and Firmware
MP = MPE/iX
MU = Multi-Platform Software
NS = NonStop Servers
OV = OpenVMS
PI = Printing and Imaging
PV = ProCurve
ST = Storage Software
TU = Tru64 UNIX
UX = HP-UX
```

Copyright 2012 Hewlett-Packard Development Company, L.P.
Hewlett-Packard Company shall not be liable for technical or editorial errors or \ omissions contained herein. The information provided is provided "as is" without \ warranty of any kind. To the extent permitted by law, neither HP or its affiliates, \ subcontractors or suppliers will be liable for incidental, special or consequential \ damages including downtime cost; lost profits; damages relating to the procurement of \ substitute products or services; or damages for loss of data, or software \ restoration. The information in this document is subject to change without notice. \ Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein \ are trademarks of Hewlett-Packard Company in the United States and other countries. \ Other product and company names mentioned herein may be trademarks of their \ respective owners.

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

Version: GnuPG v1.4.10 (GNU/Linux)

iEYEARECAAYFAk8XFPeACgkQ4B86/C0qfVngVgCfQYyXQ5WEkaKKYw3YgQWMTcMT
9tgAoMTEk1JA6mVfBpTDyJ9mGBburhfH
=1FVq
-----END PGP SIGNATURE-----

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)