

Sun Alert Notifications from Sun Summary Report dated September 17, 2005

Advisory Original Release Date: October 18, 2005

Last Revised: October 18, 2005

Number: ASA-2005-218

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Interim

Overview:

New Sun Alert Notifications from Sun Microsystems have been issued and are described as follows. Issues which have been resolved by Sun Microsystems have been indicated as such. Notifications without a resolution may have restrictions to additional information on the sunsolve.sun.com web site.

101902

Upgrading Brocade FOS From Versions Earlier than 4.2.2 May Cause Temporary Loss of Access to Storage

Date Released: 15-Sep-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101902-1>

101903

Brocade Switches With FOS 4.4.0b/4.4.0e May Panic, Reporting "Out of Memory"

Date Released: 12-Sep-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101903-1>

101905 (RESOLVED by Sun)

Security Vulnerability in Sun Java System Application Server Exposes Contents of "jar" File of Deployed Web Applications

Date Released: 13-Sep-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101905-1>

101919

In the Event of a System Panic, Data Loss may Occur if Certain Patches are Installed

Date Released: 15-Sep-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101919-1>

101926

Security Vulnerability in the Xsun(1) and Xorg Servers

Date Released: 15-Sep-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1>

The common vulnerabilities and exposures project (cve.mitre.org) has assigned the name [CAN-2005-2495](https://nvd.nist.gov/vuln/detail/CAN-2005-2495) to this issue.

Avaya System Products using Sun Microsystems: Avaya system products include an Operating System with the product when it is delivered. The Avaya **Call Management System** (CMS) and the Avaya **Interactive** Response (IR) are

taken on these products are described below.

Recommended Actions: Follow the recommended actions for each notification described below. This advisory will be updated as additional information becomes available.

<u>Sun Advisory</u>	<u>Affected S/W Version</u>	<u>Risk</u>	<u>Comments or Recommended Actions</u>
101902	NONE	None	No action required. CMS and IR are not affected; Brocade switches are not used.
101903	NONE	None	No action required. CMS and IR are not affected; Brocade switches are not used.
101905	NONE	None	No action required. CMS and IR are not affected; Sun Java System Application Server is not used.
101919	NONE	None	No action required. CMS and IR are not affected; Rev 32-35 of affected versions are not used.
101926	CMS – v9,10,11,R12,13	Low	CMS V9,10,11 R12,13 – Potentially vulnerable. A workaround is available via Avaya Services while final patches from SUN are pending
	IR - NONE	None	IR - None

Additional Information: Additional information may also be available via the Avaya support website (<http://support.avaya.com>) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH

AVAYA.

Revision History:

V 1.0 - October 18, 2005 - Initial statement issued.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.

© 2005 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.