

Sun Alert Notifications from Sun Summary Report dated April 21, 2005 (SUN-57765, SUN-57769, SUN-57773 & SUN-57776)

Advisory Original Release Date: May 13, 2005

Last Revised: May 13, 2005

Number: ASA-2005-113

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

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.

57744

Using the Reset Button on A Main System Controller May Cause Domain Outage

Date Released: 21-Apr-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57744-1>

57763 (RESOLVED by SUN)

Buffer Overflow Vulnerabilities in Sun Java System Web Proxy Server

Date Released: 19-Apr-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57763-1>

57766 (RESOLVED by SUN)

Certain Network Services Disruptions or "Spoofs" Could Occur as a Result of Possible Network Port Theft

Date Released: 18-Apr-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57766-1>

57768 (RESOLVED by SUN)

Multiple Security Vulnerabilities in Xsun and Xprt Server Font Handling

Date Released: 18-Apr-2005

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57768-1>

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 both shipped with an operating system from Sun Microsystems. Actions to be 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>
57744	NONE	None	No action required. CMS and IR are not affected; CMS and IR do not use any of the affected platforms.
57763	NONE	None	No action required. CMS and IR are not affected; CMS and IR do not use Sun Java System Web Proxy Server
57766	CMS – V9, V11, R12 and R13 IR - ALL	Low	CMS is potentially affected by this vulnerability. NOTE: You must upgrade to the latest load BEFORE installing these patches to obtain dependent patches Patches: CMS V9/V11: 116965-08 CMS R12/R13: 118305-02 IR - Patch 116965-10 will be included in the next certified patch cluster dated 5/10/05
57768	CMS – V9, V11, and R12 IR - ALL	Low	CMS - All necessary patches are in latest V9/V11/R12 loads, upgrade to receive patches. IR - Patch 108652-90 will be included in the next certified patch cluster dated 5/10/05

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 1-866-GO-AVAYA, 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 – May 13, 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.