Sun Alert Notifications from Sun Summary Report dated August 9, 2005 (SUN-101834, SUN-101841, SUN-101842, SUN-101846, SUN-101853, SUN-101864)

Advisory Original Release Date: August 17, 2005
Last Revised: September 6, 2007
Number: ASA-2005-165
Risk Level: High
Advisory Version: 2.0

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.

101834
Installing Certain Solaris Patches May Cause sshd(1M) and/or Bind Failure Issues
Date Released: 09-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101834-1

101841 (RESOLVED by Sun)
Updated Solaris 8 Patches for Apache Security Vulnerabilities
Date Released: 10-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101841-1

101842 (RESOLVED by Sun)
Security Vulnerability in the "printd" Daemon
Date Released: 08-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101842-1

101846
Vdisk Failure on a Sun StorEdge 6130 May Cause All the Volumes on the Same Controller to Become Inaccessible
Date Released: 10-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101846-1

101853
VxFS 4.0 MP2 Patches May Cause File System to not Mount during a Sun Cluster Failover
Date Released: 11-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101853-1

101864 (RESOLVED by Sun)
Multiple Security Vulnerabilities in The "MySQL" Package
Date Released: 11-Aug-2005
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101864-1

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.

Sun Advisory	**Affected S/W Version**	**Risk**	**Comments or Recommended Actions**
101834	NONE	None	No action required. CMS and IR are not affected; the affected patches are not installed.
101841	NONE	None	No action required. CMS and IR are not affected; Apache is not used.
101842	CMS All Versions IR All Versions	High High High	CMS V9, V10, V11– Install Sun patch 109320-16 or later CMS R12, R13 – Install Sun patch 113329-15 or later IR All versions – The fix for this issue was included in the February 2007 patch cluster from Avaya. Install the IR February 2007 patch cluster.
101846	NONE	None	No action required. CMS and IR are not affected; Sun StorEdge is not used.
101853	NONE	None	No action required. CMS and IR are not affected; SunCluster is not used.
101864	NONE	None	No action required. CMS and IR are not affected; MySWL is not used.

Additional Information:

Sun Security Alert 101842 has been found to affect Avaya products running Solaris 8 and 9. A vulnerability has been discovered with the "printd" Daemon that could allow an unauthenticated local or remote user to remove ANY file from the system. Avaya recommends installing the applicable SUN patch, listed above, to remediate the issue.

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 – August 17, 2005 – Initial statement issued.
V 2.0 – September 6, 2007 – Changed actions for 101842 regarding IR, and set advisory status to final.

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