A Security Vulnerability in Solaris Secure Shell (SSH) May Expose Some Plain Text From Encrypted Traffic (Sun 247186)

Original Release Date: December 23, 2008
Last Revised: December 23, 2008
Number: ASA-2008-503
Risk Level: Low
Advisory Version: 1.0
Advisory Status: Interim

1. Overview:

A new Sun Alert Notification from Sun Microsystems has been issued and is described below. Additional information about this issue may be found on the sunsolve.sun.com website, although a maintenance contract with Sun may be required to view the information.

247186
A Security Vulnerability in Solaris Secure Shell (SSH) May Expose Some Plain Text From Encrypted Traffic
Product: Solaris 9 Operating System, Solaris 10 Operating System, OpenSolaris
Category: Security
Date Released: 05-Dec-2008
http://sunsolve.sun.com/search/document.do?assetkey=1-66-247186-1

2. Avaya System Products using Solaris Secure Shell on a Solaris Operating System:

Some Avaya system products are delivered with an Operating System from Sun Microsystems. Actions to be taken on these products are described below.

Product:	Affected Version(s):	Risk Level:	Actions:
Avaya CMS	R13/R13.1, R14/R14.1	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy
Avaya IR	2.0 on Solaris 10, 3.0	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy

Recommended Actions:
For all vulnerable system products, Avaya recommends that customers restrict local and network access to the server. This restriction should be enforced through the use of physical security, firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update becomes available and can be installed.

3. Additional Information:

Additional information may also be available via the Avaya support website and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any

questions.

4. 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 BUT NOT LIMITED TO 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, INCIDENTAL, STATUTORY, 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.

5. Revision History:

V 1.0 - December 23, 2008 - 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.