

---

Sun Alert Notifications from Sun Weekly Report Dated November 18, 2006

Original Release Date: December 14, 2006

Last Revised: February 26, 2008

Number: ASA-2006-284

Risk Level: Low

Advisory Version: 2.0

Advisory Status: Final

---

## 1. Overview:

New Sun Alert Notifications from Sun Microsystems have been issued and are described below. 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](http://sunsolve.sun.com) website.

### **102622 (RESOLVED)**

A Security Vulnerability in the Java Runtime Environment Swing Library may Allow an Untrusted Applet to Access Data in Other Applets

Product: Java 2 Platform, Standard Edition

Category: Security

Date Released: 14-Nov-2006

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102622-1>

### **102677**

Certain Brocade Switches May Panic With "Watchdog threshold reached" Error

Product: Brocade SilkWorm 3850 Fabric Switch, Brocade SilkWorm 24000

Director, Brocade SilkWorm 3250 Fabric Switch, Brocade 12000 2 GB Switch,

SAN Brocade 12000 2 GB 64-port Switch, Brocade SilkWorm 3900 Switch

Category: Availability

Date Released: 13-Nov-2006

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102677-1>

### **102686**

Security Vulnerability in RSA Signature Verification Affects Java 2 Platform, Standard Edition

Product: Java 2 Platform, Standard Edition

Category: Security

Date Released: 15-Nov-2006

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102686-1>

### **102714**

Security Vulnerability With Integer Multiplication Within libXfont Affects Solaris X11 Servers

Product: Solaris 9 Operating System, Solaris 10 Operating System, Solaris 8 Operating System

Category: Security

Date Released: 14-Nov-2006

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102714-1>

**102719 (RESOLVED)**

Default Password Mistakenly Set for ALOM and SC Admin on Certain Systems

Product: Sun Fire V215 Server, Sun Fire V245 Server

Category: Availability

Date Released: 16-Nov-2006

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102719-1>

**Avaya System Products using a Sun Microsystems Operating System:**

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 those products are described below.

**Recommended Actions:**

Follow the recommended actions for the notifications described below. These advisories will be updated as additional information becomes available.

<b>Sun Advisory:</b>	<b>Affected S/W Version</b>	<b>Risk</b>	<b>Comments or Recommended Actions</b>
<b>102622</b>	CMS - V9, V11, R12, R13/R13.1  IR - 2.0 Solaris 10, Solaris 8, 1.3 Solaris 8	None  None	No action is required. IR and CMS do not utilize Java Runtime Environment (JRE).
<b>102677</b>	CMS - V9, V11, R12, R13/R13.1  IR - 2.0 Solaris 10, Solaris 8, 1.3 Solaris 8	None  None	No action is required. IR and CMS do not utilize Brocade switches.
<b>102686</b>	CMS - V9, V11, R12, R13/R13.1  IR - 2.0 Solaris 10,	None  None	No action is required. IR and CMS do not utilize Java 2.

	Solaris 8, 1.3 Solaris 8		
<b>102714</b>	CMS - V9, V11, R12, R13/R13.1  IR - 2.0 Solaris 10, Solaris 8, 1.3 Solaris 8	Low  Low	Customers with CMS V9 and V11 should install patch 119067-04. Customers with CMS R12 should install patch 112785-57 and customers with R13/R13.1 should install patch 119059-19.  Customers with IR 1.3 and 2.0 on Solaris 8 should install the latest Solaris 8 Patch Cluster or patch 119067-04. Customers with IR 2.0 and 3.0 on Solaris 10 should install the latest Solaris 10 Patch Cluster or patch 119059-19. Patch clusters are available on <a href="http://support.avaya.com">http://support.avaya.com</a> .
<b>102719</b>	CMS - V9, V11, R12, R13/R13.1  IR - 2.0 Solaris 10, Solaris 8, 1.3 Solaris 8	None  None	No action is required. IR and CMS do not utilize SunFire V215 or V245 servers.

## 2. 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.

## 3. 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.

## **4. Revision History:**

V 1.0 - December 14, 2006 - Initial Statement issued.

V 2.0 - February 26, 2008 - Updated actions for CMS and IR under Sun Alert ID 102714 and changed 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](mailto:securityalerts@avaya.com).

© 2006,2008 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.