
Solaris 10 Kernel Patches May Allow Privileged Remote Users to Gain Root Access to Files Shared by NFS Servers (Sun 103162)

Original Release Date: December 19, 2007

Last Revised: December 19, 2007

Number: ASA-2007-531

Risk Level: None

Advisory Version: 1.0

Advisory Status: Final

1. Overview:

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

103162

Solaris 10 Kernel Patches May Allow Privileged Remote Users to Gain Root Access to Files Shared by NFS Servers

Product: Solaris 10 Operating System

Category: Security, Availability

Date Released: 13-Dec-2007

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103162-1>

2. Avaya System Products using a Sun Microsystems Operating System:

Avaya system products include an Operating System with the product when it is delivered. Avaya *Call Management System* (CMS) and 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 products listed below. This advisory will be updated as additional information becomes available.

Product:	Affected Version(s):	Risk Level:	Actions:
Avaya CMS	None	None	CMS is not installed on the Solaris 10 Operating System.

Avaya IR	None	None	This issue only applies to Solaris 10 with patch 127111-05 or later installed. The affected patch is not installed or supported on IR.
----------	------	------	--

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 19, 2007 - 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.

© 2007 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.