

## HP-UX HP-UX trusted system remote unauthorized access (HPSBUX01165)

**Advisory Original Release Date:** August 29, 2005

**Last Revised:** August 29, 2005

**Number:** ASA-2005-169

**Risk Level:** Low

**Advisory Version:** 1.0

**Advisory Status:** Final

### Overview:

A new Security and Support Alert from Hewlett-Packard has been issued regarding HP-UX and is described as follows.

**HPSBUX01165** - SSRT5899 rev.0 - HP-UX trusted system remote unauthorized access

IMPACT: Remote unauthorized access

SUMMARY: A potential security vulnerability has been identified with HP-UX trusted systems where the vulnerability may be exploited to allow remote unauthorized access.

OS: HP-UX B.11.00, HP-UX B.11.11, HP-UX B.11.22, HP-UX B.11.23

URL:

<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01165>

**Avaya System Products using HP-UX:** Avaya system products include an Operating System with the product when it is delivered. The Avaya **Predictive Dialing System (PDS, formerly MOSAIX™)** is shipped with the HP-UX Operating system. Actions to be taken on this product are described below.

**Recommended Actions:** Follow the recommended actions for this notification as described below.

<u>Affected S/W Version</u>	<u>Risk</u>	<u>Comments or Recommended Actions</u>
Predictive Dialer System (PDS)	HP-UX 11.00 (PDS v12)	HP-UX 11.00 (PDS v12)– install PHCO_29249 and PHNE_17030 or subsequent patches
	HP-UX 11.11 (PDS v12)	HP-UX 11.11 (PDS v12) - install PHCO_33215 or subsequent

**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 1-800-242-2121, 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 29, 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](mailto: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.