HP-UX Perl Local Unauthorized Elevated Privileges (*HPSBUX01208*)

Advisory Original Release Date: September 13, 2005
Last Revised: September 13, 2005
Number: ASA-2005-196
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.

> ***HPSBUX01208*** *- SSRT5938 rev.0 - HP-UX perl local unauthorized elevated privileges*
> IMPACT: local unauthorized elevated privileges
> SUMMARY: A potential security vulnerability has been identified with HP-UX running perl where the potential vulnerability could be exploited by a local user to gain unauthorized elevated privileges.
> AFFECTED SOFTWARE
> HP-UX B.11.00, B.11.11, and B.11.23 running perl.
> URL:
> http://www2.itrc.hp.com/service/cki/docDisplay.do?admit=-1335382922+1126640573087+28353475&docId=HPSBUX01208

Certain versions of the Avaya™ Predictive Dialer System (PDS) are affected by this vulnerability. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0448 to this issue.

Avaya System Products using HP-UX:

Affected S/W Version	Affected S/W Versions	Comments or Recommended Actions
Predictive Dialer System (PDS)	HP-UX 11.00 (PDS v12) HP-UX 11.11 (PDS v12)	Avaya recommends customers follow the recommended actions supplied by HP and install Perl reversion D.5.8.0.G 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 - September 13, 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.