HP-UX TCP/IP Remote Denial of Service (HPSBUX01137)

Original Release Date: July 15, 2005
Last Revised: November 19, 2007
Number: ASA-2005-160
Risk Level: Medium
Advisory Version: 3.0
Advisory Status: Final

1. Overview:

Title: HP-UX TCP/IP Remote Denial of Service (HPSBUX01137)
Potential Impact: Denial of Service by remote unauthorized user
Summary: A potential security vulnerability has been identified with HP-UX running TCP/IP (IPv4). This vulnerability could be remotely exploited by an unauthorized user to cause a Denial of Service (DoS). The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2005-1192 to this issue.
Affected Versions:HP-UX 11.00, 11.11, 11.23

2. Avaya System Products with HP-UX TCP/IP:

Product:	**Affected Version(s):**	**Risk Level:**	**Actions:**
Avaya Predictive Dialer	HP-UX 11.00, 11.11, 11.23	Medium	Install PHNE_33159

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 - July 15, 2005 - Initial Statement issued.
V 2.0 - April 16, 2007 - Updated statement issued providing patch solution.
V 3.0 - November 19, 2007 – Updated 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.