
HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02294)

Original Release Date: December 18, 2007

Last Revised: December 18, 2007

Number: ASA-2007-529

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

1. Overview:

Title: HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02294)

Potential Impact: Remote Denial of Service (DoS)

Summary: A potential security vulnerability has been identified with HP-UX applications running DCE such as Software Distributor (SD). The vulnerability could be exploited remotely to create a denial of service (DoS). The vulnerability could be exploited remotely to execute arbitrary code. The Common Vulnerabilities and Exposures project (cve.mitre.org) assigned the name [CVE-2007-6195](https://cve.mitre.org/cve/2007/6195) to this issue.

Affected Versions: HP-UX B.11.11 and B.11.23

2. Avaya System Products with HP-UX running DCE:

Product:	Affected Version(s):	Risk Level:	Actions:
Avaya Predictive Dialer	All	Low	Install patch PHSS_36004 or subsequent
Avaya Proactive Contact	All	Low	Install patch PHSS_36004 or subsequent

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 18, 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.