Update to Hewlett-Packard Security Advisories (HPSBUX0302-241, HPSBUX01088, HPSBUX01061, HPSBUX01111 and HPSBUX01113)

Advisory Original Release Date: February 4, 2005
Last Revised: February 4, 2005
Number: ASA-2005-032
Risk Level: Medium
Advisory Version: 1.0

Advisory Status: Final

Overview:
New Security and Support Alerts from Hewlett-Packard have been issued regarding HP-UX and are described as follows.

> ***HPSBUX0302-241*** - SSRT3472 rev.2, rev.3 HP-UX stmkfont potential unauthorized access
> IMPACT: Potential unauthorized access by a local user.
> SUMMARY: There is a potential buffer overflow in /usr/bin/stmkfont which could be exploited by a local user to allow unauthorized access.
> OS: HP-UX B.10.20, B.10.26, B.11.00 and B.11.04.
> Release Date: Tue Jan 25 6:00:03 EST 2005
> URL:
> http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0302-241
>
> ***HPSBUX01088*** - SSRT4807 rev.1 HP-UX stmkfont local unauthorized privileged access
> IMPACT: local unauthorized privileged access
> SUMMARY: A potential security vulnerability has been reported with the HP-UX stmkfont program. This vulnerability can be exploited to allow local unauthorized access to resources owned by group 'bin.'
> OS: HP-UX B.11.00, B.11.04, B.11.11, B.11.22, B.11.23
> Release Date: Tue Jan 25 6:00:03 EST 2005
> URL:
> http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01088
>
> ***HPSBUX01061*** - SSRT4773 rev.3 HP-UX xfs and stmkfont remote unauthorized access
> IMPACT: remote unauthorized access
> SUMMARY: Potential security vulnerabilities have been reported with HP-UX running xfs and stmkfont. These vulnerabilities can be exploited to allow remote unauthorized access to resources owned by group 'bin.'
> OS: HP-UX B.11.00, B.11.04, B.11.11, B.11.22, B.11.23
> Release Date: Tue Jan 25 6:00:03 EST 2005
> URL:
> http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01061
>
> **HPSBUX01111** - SSRT5900 rev.0 HP-UX TGA daemon remote Denial of Service (DoS)

IMPACT: remote Denial of Service (DoS)
SUMMARY: A potential security vulnerability has been identified with HP-UX running the TGA daemon, where certain network traffic could be used to create a Denial of Service (DoS). The vulnerability is remotely exploitable.
OS: HP-UX B.11.04 with Virtualvault 4.7, 4.6 or 4.5.
Release Date: Thu Jan 27 6:00:02 EST 2005
URL:
http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01111

HPSBUX01113 - SSRT5902 rev.0 Apache 1.3 on VirtualVault potential remote Denial of Service (Do
IMPACT: Remote Denial of Service (DoS) and execution of arbitrary code.
SUMMARY: Two security vulnerabilities have been reported in Apache HTTP server (http://httpd.apache.org/) versions prior to Apache 1.3.33 that may allow a Denial of Service (DoS) attack and execution of arbitrary code. (*CAN-2004-0492, CAN-2004-0940*)
OS: HP-UX B.11.04 with VirtualVault 4.7, Virtualvault 4.6, or VirtualVault 4.5, and HP Webproxy A.02.10 and A.02.00 only.
Release Date: Fri Jan 28 6:00:03 EST 2005
URL:
http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01113

Avaya System Products using Sun Microsystems: 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: PDS v9, v11 and H-UX v11.00 based v12 platforms contain X-Windows related binaries that could allow local escalation of user privileges to user 'bin' if a user has access to these X-Windows binaries. These vulnerabilities can be fixed by either applying the patches available from HP or deleting the following vulnerable binaries:

- */usr/bin/stmkfont*
- */usr/bin/X11/xfs*

No actions are required for HPSBUX01111 or HPSBUX01113 as they do not impact PDS platforms.

HP Advisory	**Affected S/W Version**	**Risk**	**Comments or Recommended Actions**
HPSBUX0302-241	All PDS v9 and v11 platforms and HP-UX v11.00 based V12 platforms have a vulnerable version of stmkfont installed. PDS v12 platforms based	MEDIUM	Certain versions of PDS platforms ship with X-Windows installed and include a vulnerable stmkfont binary. X-Windows is not required for operation of PDS platforms, and Avaya recommends removal of this

	HP-UX 11.11 do not include this package are not effected		binary or and/or application of the patches available from HP to fix this vulnerability.
HPSBUX01088	All PDS v9 and v11 platforms and HP-UX v11.00 based V12 platforms have a vulnerable version of stmkfont installed. PDS v12 platforms based HP-UX 11.11 do not include this package are not effected	MEDIUM	Certain versions of PDS platforms ship with X-Windows installed and include a vulnerable stmkfont binary. X-Windows is not required for operation of PDS platforms, and Avaya recommends removal of this binary or and/or application of the patches available from HP to fix this vulnerability.
HPSBUX01061	All PDS v9 and v11 platforms and HP-UX v11.00 based V12 platforms have a vulnerable versions of stmkfont and xfs installed. PDS v12 platforms based HP-UX 11.11 do not include these packages are not effected	MEDIUM	Certain versions of PDS platforms ship with X-Windows installed and include vulnerable *stmkfont* and *xfs* binaries. X-Windows and associated services are not utilized on PDS platforms, so this vulnerability is limited to a local privilege escalation unless X-Windows is manually started. X-Windows is not required for operation of PDS platforms, and Avaya recommends removal of vulnerable binaries or and/or application of the patches available from HP to fix this vulnerability.
HPSBUX01111	None	NONE	This vulnerability only impacts HP-UX 11.04 and no PDS platforms utilize HP-UX 11.04
HPSBUX01113	None	NONE	This vulnerability only impacts HP-UX 11.04 and no PDS platforms utilize HP-UX 11.04

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 1-866-GO-AVAYA, 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 – February 4, 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.