Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN # PSN004154u

Original publication date: 27-Feb-14. This is Issue #03, published date: 3-Mar-14. Severity/risk level Medium Urgency when convenient

Name of problem Avaya 96x1 and B189 Endpoint Command Injection, Memory Modification and Code Execution Vulnerabilities

Products affected

Avaya IP Endpoints affected:

Product:	**Affected Version(s):**	**Risk Level:**	**Actions:**
Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones	6.3.1.21 and earlier SIP software	Medium	Upgrade to 6.3.1.22 (May 15th, 2014) GA or newer, available on the Avaya Support website.
Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones	6.3.1.51 and earlier H.323 software	Medium	Upgrade to 6.4.0.14 (June 2, 2014) GA or newer, available on the Avaya Support website.
Avaya B189 IP Conference Phone	1.0.0.22 and earlier H.323 software	Medium	Upgrade to 1.0.1.08 (June 8, 2014) GA or newer, available on the Avaya Support website.

Problem description

1. Overview:

Avaya's IP endpoints retrieve an upgrade and settings file from an HTTP server during boot up. The HTTP server IP address is set up in the endpoint either via DHCP or manually by entering a special key sequence with a password on the key pad. Modifications to the upgrade and settings files require user access and permissions on the HTTP server. Software on the IP endpoints parses the contents of these files and is only executed while reading these files.

A vulnerability exists in this parsing software, which could potentially execute arbitrary shell commands as root, allowing arbitrary changes to the kernel and all applications on the phone.

A second vulnerability exists in the parsing software for endpoints using SIP signaling. This vulnerability could potentially cause a buffer overflow on the stack, allowing arbitrary changes to memory and execution of arbitrary code as root.

Resolution

See table in the “Products Affected” section of this PSN.

Workaround or alternative remediation

n/a

Remarks

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions	Service-interrupting?
n/a	No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

ASA_2014_099 – https://support.avaya.com/security

Avaya Security Vulnerability Classification

Medium

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF 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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.