

Avaya P330/P130 and G700 possible denial of service vulnerability

Advisory Original Release Date: June 18, 2003

Last Revised: January 3, 2005

Number: ASA-2005-001

Risk Level: Medium

Advisory Version: 2.0

Advisory Status: Final

Overview:

The Avaya P330/P130 and G700 products with SW version lower than 4.0.were found to be susceptible to service delays when trying to connect to certain TCP/UDP ports.

Description:

When ports TCP 4000 and UDP 4501 on the P330/P130 switch and the G700 Media Gateway receive packets of particular size and value the device will reset. The affected ports are typically blocked at a firewall.

Note that this advisory was originally release without an ASA-number assigned to it. For improved tracking, this advisory has been assigned the ASA number indicated above.

Recommended Action:

· For the **P330**, please upgrade to software version 4.1, this will eliminate the vulnerability. Upgrade for the various P330 products can be found at **support.avaya.com**. Look for firmware and software downloads for the P330 Stackable Switching System. Firmware upgrades are directly available from the following hyperlinks:

- o [\(5\) Avaya P330 Layer 2 Product - Version 4.1. \(P333T/P334T/P332MF, P333T-PWR\)](#) (2.45 MB)
- o [\(9\) Avaya P330 Multilayer Product - Version 4.1 \(P332G-ML, P332GT-ML, P334T-ML\)](#) (3.74 MB)
- o [\(10\) Avaya P330 Multilayer Product - Version 4.1 \(P333R\)](#) (3.35 MB)
- o [\(11\) Avaya P330 Multilayer Product - Version 4.1 \(P333R-LB\)](#) (4.25 MB)

· For the **P130**, please upgrade to software version 2.14, this will eliminate the vulnerability. This upgrade is available at **support.avaya.com**. Look for firmware and software downloads for the P130 Workgroup Switch. A firmware upgrade is available from the following hyperlink:

- o [Avaya P130 Workgroup Switch - Version 2.14](#) (2.16 MB)

· A firmware upgrade for the G700 is planned to be available in February 2005. Until a upgrade is released for the G700, block traffic at the firewall which may be targeted for the aforementioned ports. Do not allow inbound connections from untrusted sources through the firewall to the device.

List of Avaya products affected:

Affected Product	Affected S/W Version	Info/Status
Avaya P33x	Versions below 4.0	Follow recommended actions above.
Avaya P13X	All versions	Follow recommended actions above
G700 Media Gateway	Versions below 4.0	Follow recommended actions above. A firmware upgrade is planned to be available for G700 in February 2005

Acknowledgement: Avaya would like to thank Jacek Lipkowski (sq5bpf@andra.com.pl) from [ANDRA Co. Ltd.](#) For bringing the vulnerability to the attention of Avaya.

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 - June 17, 2003 - Initial statement issued.
- V 2.0 - January 3, 2005 - Advisory Updated with more current release

information.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.

© 2004 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.