

Security Advisory Relating to Denial of Service Vulnerability on Polycom® SoundPoint® IP and SoundStation® IP Phones

This technical bulletin describes the security advisory as it relates Polycom SoundPoint IP and SoundStation IP phones.

This information applies certain SoundPoint IP and SoundStation IP phones running Polycom UC software versions 3.3.1 and earlier.

Symptom

Polycom SoundPoint IP and SoundStation IP phones may be vulnerable to Denial of Service (DOS) attacks when used in some configurations. Sending HTTP GET requests with a broken authorization header can produce a device restart under some circumstances in certain models of SoundPoint IP and SoundStation IP phones.

Cause

The previous integrated Web server had no proper input validation for these types of HTTP headers. The new Web server does.

Workaround

Phone system administrators concerned about this attack vector can disable the Web management option on their phones to completely avoid any risk of malicious device restarts. This will not affect the regular usage of the phone. For instructions on how to disable the Web interface, please consult the Polycom UC Software Administrator's Guide at http://support.polycom.com/global/documents/support/setup_maintenance/products/voice/spip_ss_ip_Admin_Guide_UCS_v3_3_0.pdf

Status

At this time, Polycom is developing hot fixes to the SIP 3.2.4 and UCS 3.3.1 releases that will remove the vulnerability. These hot fixes will be available from the Polycom support website by February 16, 2011. The central location for downloading software releases is http://downloads.polycom.com/voice/voip/sip_sw_releases_matrix.html.

Please consult the table below to determine if your phone is affected and if so, which update to install.

Phone Model	Update Needed
SoundPoint IP models – 300, 301, 500, 501, 600, and 601	These models are unaffected and do not require a patch for this issue.
SoundStation IP 4000	This model is unaffected and does not require a patch for this issue.
SoundPoint IP 430	spip_ssip_vvx_3_2_4B_release_sig_split.zip or spip_ssip_vvx_3_2_4B_release_sig_combined.zip
SoundPoint IP models – 320, 321, 330, 331, 335, 450, 550, 560, 650, and 670	spip_ssip_vvx_3_2_4B_release_sig_split.zip or spip_ssip_vvx_3_2_4B_release_sig_combined.zip or UC_Software_3_3_1F_release_sig_split.zip or UC_Software_3_3_1F_release_sig_combined.zip
SoundStation IP models – 5000, 6000, and 7000	spip_ssip_vvx_3_2_4B_release_sig_split.zip or spip_ssip_vvx_3_2_4B_release_sig_combined.zip or UC_Software_3_3_1F_release_sig_split.zip or UC_Software_3_3_1F_release_sig_combined.zip
VVX 1500	This model is unaffected and does not require a patch for this issue.

Any customer using one of the affected products that is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or log a ticket online at <http://support.polycom.com/PolycomService/home/home.htm>



Trademarks

©2011, Polycom, Inc. All rights reserved.

POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.