Polycom® HDX® Security Update
Frequently Asked Questions

This document provides information regarding security exploitations in Polycom HDX software prior to version 3.1.1.3, details to understand whether or not your systems are vulnerable, recommended remediation actions, and availability of additional security information.

Which versions of HDX software are vulnerable?
All HDX versions prior to 3.1.1.3 are vulnerable.

Is this being exploited in the wild (i.e. still an active threat to customers)?
Yes.

How do I know if my HDX system has been attacked?
The HDX system will hang (freeze) while displaying a splash screen and not complete the boot process that opens the Polycom video application.

If my HDX system is attacked how do I get it fixed?
Customers experiencing this situation should contact Polycom Support at 1-800-POLYCOM. Support will need remote access to the HDX's IP address, and will be able to restore the device to operation.

What should I do to prevent my HDX system from being attacked?
Polycom recommends that all customers immediately upgrade to HDX version 3.1.1.3. Polycom has fixed these issues in HDX version 3.1.1.3, which is no longer vulnerable to this exploit.

What security recommendations does Polycom offer?
Secure video conferencing is a priority for Polycom, and we have security features across our full range of solutions. All of our solutions - from endpoints to infrastructure – come with features that meet the most stringent industry standards. When your use of video conferencing systems is consistent with best practices, these features can ensure your audio, video and data traffic will remain fully secure as they pass across the network.

For on-going information about security on Polycom products please visit our security information web site at: www.polycom.com/security which provides best security practice recommendations and also links to the Security Center where security advisories are posted.

Additionally in keeping with security best practices customers should always do the following:

- Change the default password
- Use a password on their video conferencing systems
- Disable protocols and interfaces that are not used such as telnet
- If the system is used only when people are in the room Polycom recommends disabling the 'auto answer' functionality – allowing users to manually answer incoming calls and to consider disabling remote control of the local camera

May 16, 2013