

Media Update:

New York Times Article “Cameras May Open Up the Board Room to Hackers”

What is the news?

On Monday January 23, 2012, the New York Times ran an article calling attention to potential security vulnerabilities with auto-answer functionality in video conferencing equipment naming Polycom, Cisco, LifeSize and Sony specifically. The article comments that auto-answer for video calls is enabled by default only in Polycom systems, potentially exposing clients to unnecessary risk. Both Polycom and senior analysts at Wainhouse respond in the article stating that security mechanisms and protocols exist to block unnecessary risk when deployed properly.

Click here for hyperlink to New York Times Article: “Cameras May Open Up the Board Room to Hackers”
http://www.nytimes.com/2012/01/23/technology/flaws-in-videoconferencing-systems-put-boardrooms-at-risk.html?_r=1&scp=1&sq=video%20conferencing&st=cse

Polycom Perspective

There is no debate that protecting corporate information and privacy is absolutely critical in today’s business climate. As such, Polycom takes a very pro-active approach to providing our customers a range of security options based on their needs. This article serves as a reminder of just how important it is for our customers and partners to take measures to protect their video conferencing systems from outside risks. While the article does point to one potential area of exposure for videoconferencing systems, it is imperative that we communicate to our customers and partners that our systems are secure when deployed properly. Specifically speaking, Polycom offers robust security features and policies to help protect our clients’ privacy including:

Key Security, Call Control Features and Best Practices

- Enable do-not-disturb
- Manual answer/mute auto-answer calls (i.e., disable auto-answer)
- Disable far-end camera control
- Enable AES encryption of media stream
- Automatic TLS protocol support for signaling security
- Deploy video conferencing and telepresence systems within the corporate firewall
- Use gatekeepers and video border proxies for remote access

Key Security Certifications

Polycom solutions underwent the most stringent tests via a certified third party to ensure maximum level security for even the highest and most secure areas within our government. Certifications obtained include:

- FIPS 140-2 Validation
- Joint Interoperability Test Command (JITC) Certification
- Type 1 COMSEC and Classified Service and Support
- IPv6 Certification
- Unified Communications Approved Products List (UC APL) Certification

However, even the world’s best security countermeasures cannot possibly protect our customers if they are not implemented by the customer. Our deployment documentation encourages our customers and partners to take pro-active action in the form of security assessments, audits and implementing best practices across their existing infrastructure. For those customers or partners that do not have the in-house capabilities to perform these types of audits please remind them that Polycom offers a full suite of consulting and assessment services to help our customers deploy a secure solution.

Frequently Asked Questions

Q: Why is the Polycom auto-answer feature defaulted to the “allow” setting?

A: The auto-answer feature is currently set in the default “allow” position to provide a simplified user experience when conducting point-to-point video calls as well as for administrators to easily deploy and test the equipment remotely. This functionality is currently not enabled if the dialed party is already active on a conference call using the internal bridge of the HDX.

Q: Can end users change the auto-answer status during installation?

A: Yes, however, they would need the administrator password to do so (provided the system was configured with one at setup).

Q: Can IT departments lock the auto-answer status?

A: Yes, this can be configured by CMA provisioning, remotely via the Web GUI or directly via the HDX keypad interface.

Q: Is there any visual indicator in room for Auto-Answer for incoming Video calls?

Yes, the system wakes up, the screen(s) light up, and the camera moves to forward position. The user would also see an on-screen message of an incoming call.

Q: if no one is in the room when the camera wakes up, how can we make sure that someone can’t remotely monitor the room?

A: Polycom offers a camera lens cover that will prevent the camera from generating any video image.

Q: Will the auto-answer default be changed?

A: Polycom product management is currently evaluating this decision.

Additional Resources

Deployment guide: Disabling Auto-Answer in the Polycom HDX

For customers asking how to check and disable the auto-answer feature, please refer them to the attached guide “Disabling Auto-Answer in the Polycom HDX”. This simple guide provides step-by-step instructions to check and disable the auto-answer feature.

Best Practices for Securely Deploying Polycom Video Conferencing equipment

For customers that want to learn more about best practices for securely deploying Polycom video conferencing equipment, please refer them to our security webpage at www.polycom.com/security

Polycom Security Certifications

http://www.polycom.com/solutions/industry/federal_government/certification_accreditation.html

Summary of Key points

- Raising the awareness of video security issues is a good thing for our customers
- Polycom video conferencing systems are secure when deployed using best practices
- Encourage customers to do a self-audit of their systems to identify potential security policy vulnerabilities using attached guide
- Encourage partners to engage with their customers to identify potential security policy issues with their current deployment
- Direct customers and partners to Polycom professional services for a more thorough network assessment if required

Additional Contacts

Shawn Dainas	Corporate Communications	Shawn.dainas@polycom.com	+1 (925) 924-5676
Chris Thorson	Product Marketing	Chris.thorson@polycom.com	+1 (720) 872-7532
Ted Doty	Product Management	Ted.doty@polycom.com	+1 (512) 681-4139

About Polycom

Polycom is the global leader in standards-based unified communications (UC) solutions for telepresence, video, and voice, powered by the Polycom® RealPresence™ Platform. The RealPresence Platform interoperates with the broadest range of business, mobile and social applications and devices. More than 400,000 organizations trust Polycom solutions to collaborate and meet face to face from any location for more productive and effective engagement with colleagues, partners, customers, specialists, and prospects. Polycom, together with its broad partner ecosystem, provides customers with the best TCO, scalability, and security for video collaboration, whether on-premises, hosted or cloud-delivered. Visit www.polycom.com or connect with Polycom on Twitter, Facebook, and LinkedIn.