SECURITY BULLETIN – Worldwide H.323 and SIP Botnet Calling Video Systems
Version 1.6

DATE PUBLISHED: January 14th, 2020

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

Please Note: Poly takes the security of our customers and our products seriously. This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:

https://support.polycom.com/content/support/security-center.html

Situation Summary

A "botnet", or mass group of systems on the Internet under the control of one or several malicious entities, is being used to place calls to any device on the Internet that can meaningfully respond to an H.323 or SIP call. This means endpoints, bridges, MCU's, gatekeepers, firewalls, proxies, etc. might all be called by the botnet.

The purpose of the botnet is unclear, although toll fraud is usually the purpose behind such broad sweeps against systems that speak a specific communications protocol. The systems used in the botnet are, as is typical with this method, innocent third-party hosts whose owners are most likely unaware are a part of the botnet.

The botnet can successfully be run against all H.323 and SIP systems it finds on the Internet, and is presumably noting which systems respond to calls for future attacks.

*One particular botnet advertises itself by the fact that it seems to consistently use "*h323-ID = 'cisco'". The name appears to be unrelated to anything in the real world, and is rather a way of adding seeming legitimacy to the H.323 botnet. Others seen more recently are simply using an IP address for the h323-ID.

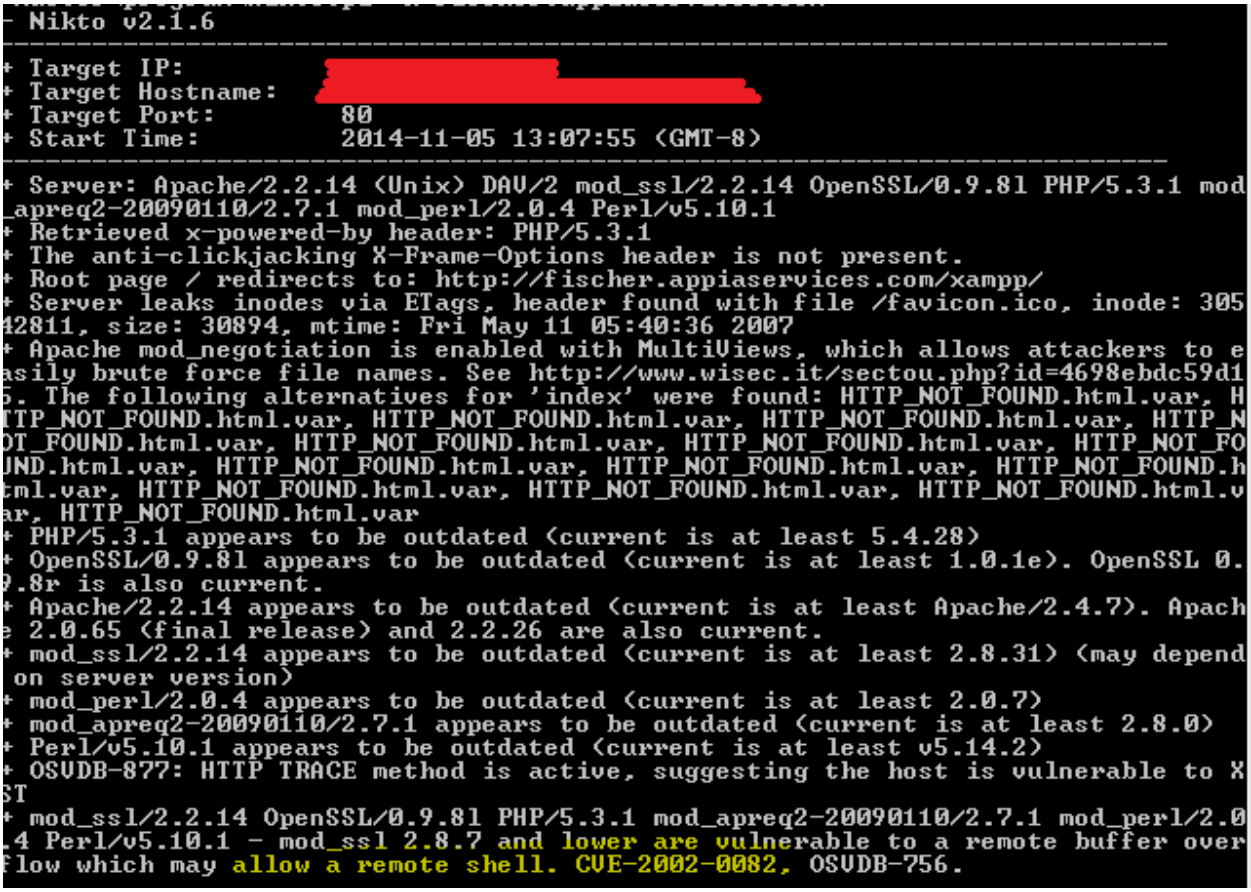
Situation Details

The botnet appears to be at least partially (probably mostly) comprised of web servers around the Internet, all of which appear to be operating below recommended security patch levels. Such systems are owned by innocent third parties who do not patch their systems to current levels. The attackers first use known security flaws to compromise such systems, and then insert code that dials H.323 and SIP systems and reports back to the individual(s) who created this illegal system ("bot master" and "bot herder" are the normal terms for the one(s) in control of the botnet).

Every system we have been able to analyze (but one) conforms with this model. One of the IP addresses used to call H.323 systems was analyzed and is shown below. The one system that did not conform with the under-patched web server model was an instance of FreePBX – most likely compromised in a similar manner for identical purposes.

From the perspective of the Internet, this is just a random web server whose owner failed to patch things when known vulnerabilities were announced (we had permission to scan). Such systems might be behind on patching Apache or OpenSSL or other similar modules. This one (as reported by Nikto, a free vulnerability scanner) has a vulnerability from 2002 among its many vulnerabilities.

Again, this is NOT a "bad guy" system. This is a third-party web server, poorly maintained, compromised by the attacker(s), and then loaded with the software that is performing the calls:



Impact and Risk

Since the attack is so widespread, since its purpose cannot be truly uncovered, and since each target network is different both in purpose and in layout, no one statement can be made about impact and risk. As noted above, botnets that dial communication protocols over and over to as many hosts as possible are quite likely looking for a means to conduct toll fraud – dialing calls through third-party systems, without the consent of the owners of those third-party systems.

General Mitigations

The challenge with these scenarios is that the target hosts (all H.323 and SIP-listening devices) are doing exactly what they are set up to do: answering calls. Polycom products are not

vulnerable to anything in this situation. Mitigations to relieve the burden presented by these non-stop calls therefore come in the form of adding some ability to discern desired calls from undesired calls.

Whitelisting is the most common method for separating the good calls from the bad. In an environment where all of the “good guys” are known, it is best to simply create whitelists comprised of those addresses, and to deny all inbound calls NOT from those addresses.

Other times blacklists can be grown and maintained, blocking each of the botnet callers as it is logged and confirmed to be a “bad guy”.

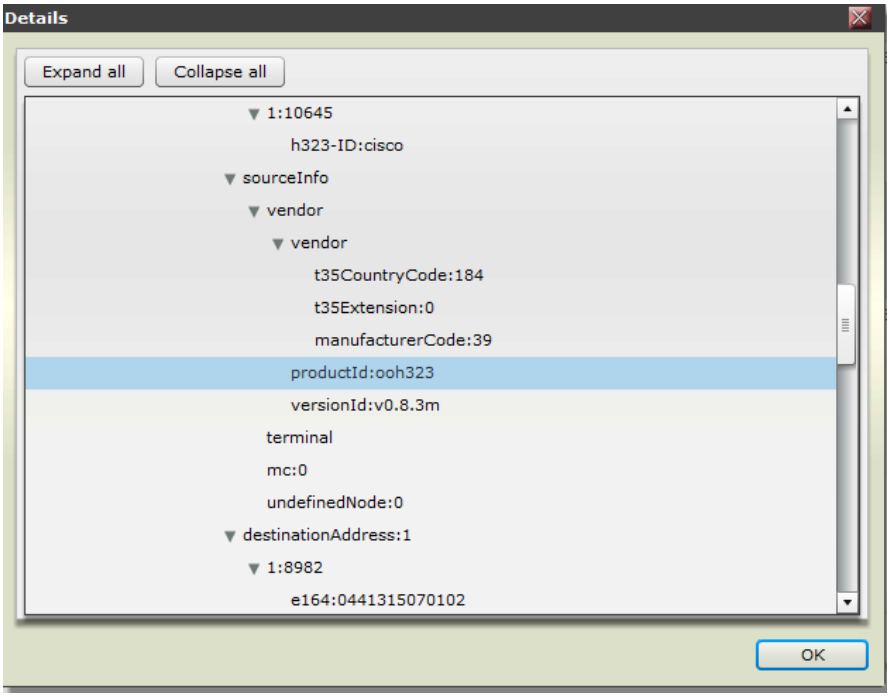
The initial botnet has consistently populated two key H.323 fields with the same information.

H.323 Alias Value: (h323-ID = “cisco”)
Vendor Product ID Field: (productId = “ooh323”)

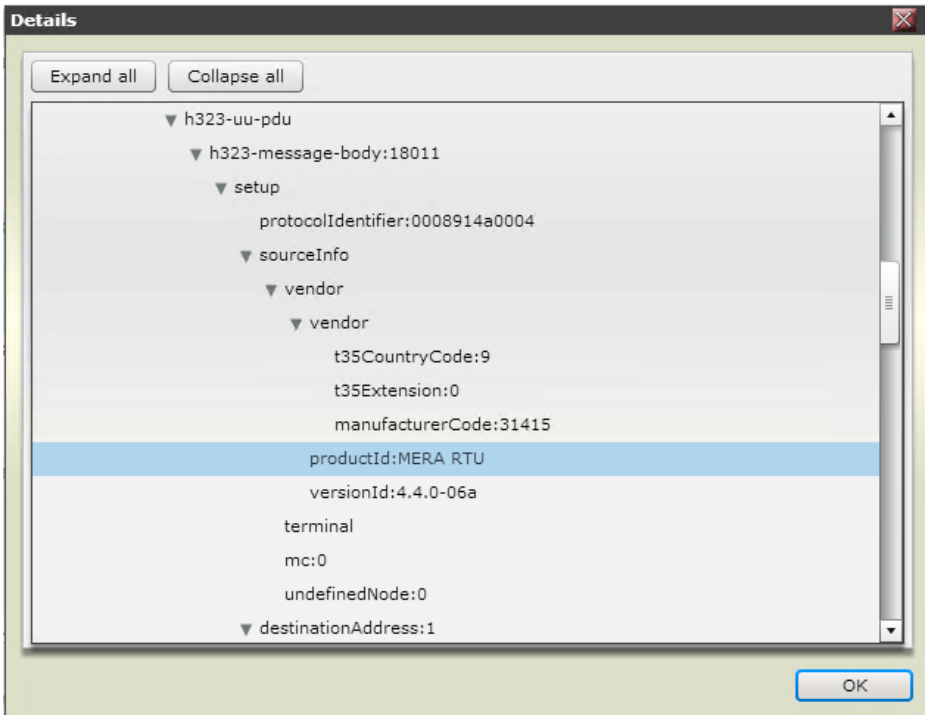
A newer variant has changed this, using an IP address for its h323-ID field but consistently populates the productId field with “MERA RTU”.

H.323 Alias Value: (h323-ID = random IP address)
Vendor Product ID Field: (productId = “MERA RTU”)

The below RPAD screenshot taken from an RPAD management interface shows both fields from the initial botnet findings:



The latest variant of the botnet can be seen using “MERA RTU” in the RPAD screenshot below:



Solution

Firewalls:

Polycom cannot give advice on specific firewall configurations or specific firewalls. Those who have a third-party firewall as their defense against incoming H.323 calls should consult with their firewall and/or security experts before implementing any of the high-level recommendation in this advisory.

H.323 is not traditionally a firewall-friendly protocol. H.323 uses both UDP and TCP over a range of ports both static and dynamic. Firewalls that support H.323 natively include special rules or modules to deal with the nuances of the H.323 protocol. Such firewalls might be able to use the field information above in the form of rules or ACL’s.

Alternatively, a firewall can come at the problem with more traditional IP-based whitelisting or blacklisting techniques.

RealPresence Access Director (RPAD):

RPAD administrators can make rules to enable blocking for the two fields listed above.

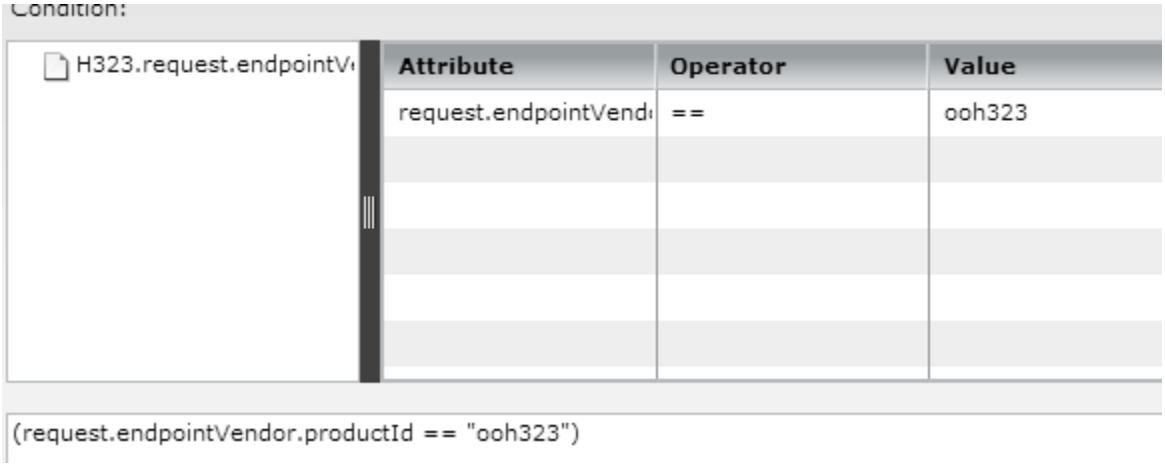
The since the release of software version 4.2.2, RPAD improves these rules and administrators should ensure they’re running this or later versions.

H.323

There are several malicious H.323 agents that can cause problems for customer environments. The table below lists some of the more common agents.

Name	Attribute	Operator	Value
ooh323	request.endpointVendor.productId	==	ooh323
MERA RTU	request.endpointVendor.productId	==	MERA RTU
cisco	request.srcAlias.fist323-ID	==	cisco

The rule for Product ID of “ooh323” is shown here below. Similar rules should be set for other agents.



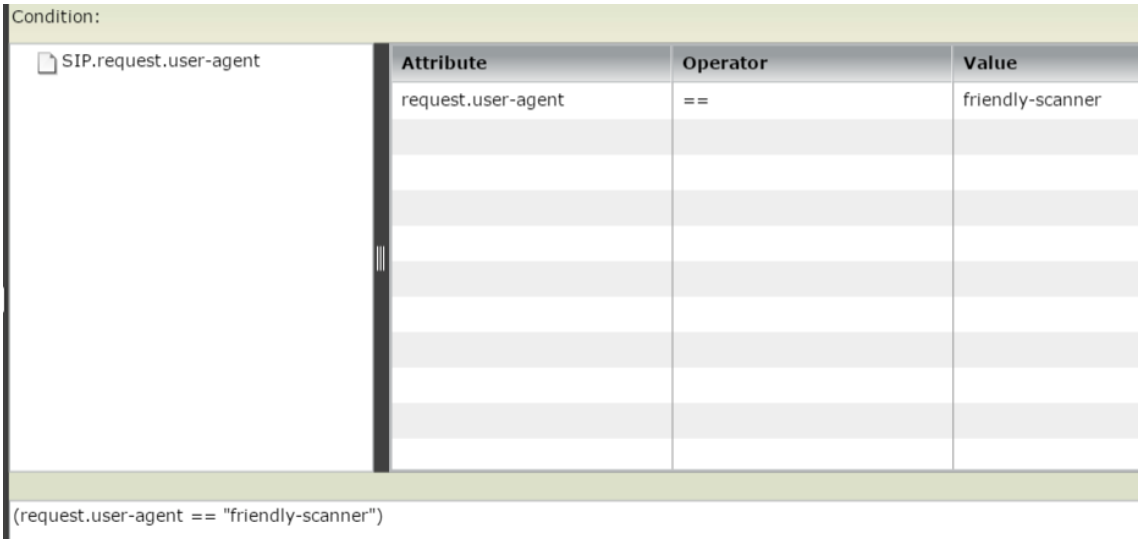
SIP

There are a growing number of malicious SIP agents that can cause problems with customer environments. The table below lists some of the more common malicious SIP agents.

Agent Name	Attribute	Operator	Value
Friendly-scanner	request.user-agent	==(case-insensitive)	Friendly-scanner
PBX	request.user-agent	==(case-insensitive)	PBX
Sipvicious	request.user-agent	==(case-insensitive)	Sipvicious
Voip	request.user-agent	==(case-insensitive)	Voip
Sipcli.*	request.user-agent	Matches	(S|s)(I|i)(P|p)(C|c)(L|l)(I|i).*
Pplsip	request.user-agent	==(case-insensitive)	Pplsip
VaxSIPUserAgent.*	request.user-agent	Matches	V|v)(A|a)(X|x)(I|i)(P|p)(U|u)(S|s)(E|e)(R|r)(A|a)(G|g)(E|e)(N|n)(T|t).*
Asterisk.*	request.user-agent	Matches	A|a)(S|s)(T|t)(E|e)(R|r)(I|i)(S|s)(K|k).*
SIPscan.*	request.user-agent	Matches	S|s)(I|i)(P|p)(S|s)(C|c)(A|a)(N|n).*
eyeBeam.*	request.user-agent	Matches	E|e)(Y|y)(E|e)(B|b)(E|e)(A|a)(M|m).*
VaxIPUserAgent.*	request.user-agent	Matches	V|v)(A|a)(X|x)(S|s)(I|i)(P|p)(U|u)(S|s)(E|e)(R|r)(A|a)(G|g)(E|e)(N|n)(T|t).*
Linksys/PAP2T-5.1.6	request.user-agent	==(case-insensitive)	Linksys/PAP2T-5.1.6
VoIP v11.1.2	request.user-agent	==(case-insensitive)	VoIP v11.1.2
xlite.*	request.user-agent	Matches	X|x)(L|l)(I|i)(T|t)(E|e).*

Cisco-SIPGateway/IOS-12.x	request.user-agent	==(case-insensitive)	Cisco-SIPGateway/IOS-12.x
FreePBX 1.8	request.user-agent	==(case-insensitive)	FreePBX 1.8
MizuPhone	request.user-agent	==(case-insensitive)	MizuPhone
AVM FRITZ!Box.*	request.user-agent	Matches	(A|a)(V|v)(M|m)("")(F|f)(R|r)(I|i)(T|t)(Z|z)(!)(B|b)(O|o)(X|x).*

The rule for SIP agent “friendly-scanner” is shown here below. Similar rules should be set for other malicious SIP agents.



Detailed information about enabling and activating rules in RPAD is available in Appendix A at the end of this document.

Video Border Proxy (VBP):

VBP version 11.2.20 has fixed the issue without need for any configuration changes. This version disables fastStart on the WAN side when the call originates from a non-registered client.

This change appears to reduce the nuisance factor of the H.323 botnet without the need for configuration changes.

Contact

Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:

https://support.polycom.com/content/support/security-center.html For the latest information.

You might also find value in the high-level security guidance and security news located at:

https://support.polycom.com/content/support/security-center.html

Revision History

DRAFT 1.0 – Original publication: November 6, 2014. RPAD configurations given with lighter reference to VBP.

Version 1.0 – Removed DRAFT status, cleared for public consumption, provided detail on VBP upgrade.

Version 1.1 – Clarification on advisory/bulletin differences and inclusion of *h323-ID = "cisco"* string earlier in the document.

Version 1.2 – Updated bulletin to address current attacks and defense configurations for "MERA RTU".

Version 1.3 – Updated bulletin to address current attacks and defense configurations for H.323 and SIP.

Version 1.4 – Updated bulletin to add additional H.323 and SIP agents.

Version 1.5 – Updated bulletin to add additional H.323 and SIP agents.

Version 1.6 – Corrected some settings and updated format for Poly.