SHA1 Deprecation Impacts

Technical Notification 100093

Microsoft announced late in 2013 that the company would deprecate SHA1 support for the Windows platform completely effective January 1, 2017 and that all code signing would use only SHA2 algorithms effective January 1, 2016.

Subsequent announcements by Google to also deprecate SHA1 triggered many well-known Certificate Authorities to also implement or further advertise their security policies and cease issuing SHA1 encrypted certificates with validity periods beyond January 1, 2016.

In addition, many code-signing Root Certificate Authorities (CAs) and their intermediaries have since been re-issued to use newer SHA2 algorithms.

Older Polycom SoundPoint IP and SoundStation IP phones that do not support the newer SHA2 encryption schemes are impacted.

This technical notification applies to the following Polycom phones:

- SoundPoint IP 300, 301, 320, 321, 330, 331, 335, 430, 450, 500, 501, 601, 650, 670
- SoundStation IP 4000, 5000, 6000, 7000
- VVX 101, 201, 300, 310, 400, 410, 500, 600, 1500

Affected Phone Models

SHA2 support was first introduced to the Polycom SPIP, SSIP, and VVX phones in UC Software 4.0.0.

Due to this minimum required software version, the following legacy phone models are unable to upgrade to a version capable of SHA2 support:

SoundPoint IP 300, 301, 320, 330, 430, 500, 501, 601

SoundStation IP 4000

The following models may be upgraded to the required minimum of UC Software 4.0.x:

SoundPoint IP 321, 331, 335, 450, 650, 670

SoundStation IP 5000, 6000, 7000

VVX 1500

The following models are not affected and have always supported the required SHA2 algorithms:

VVX 101, 201, 300, 310, 400, 410, 500, 600

Polycom Shipping Configurations

Refer to EA75429 for all current shipping configurations at the time of this writing.

As advised in EA75429, all Polycom VVX, SPIP, and SSIP phones are shipped with a UC Software version that is SHA2 compliant.

Impact and Mitigations

Impact:

The most immediate impact is that upon replacement of any Provisioning or Call Server certificate with a SHA2 signed certificate, any phone making use of the HTTPS or SIP over TLS protocols that does not meet the minimum UC Software version will be unable to successfully negotiate its TLS handshake and will fail to provision software and configuration or fail to establish a SIP signaling connection.

The result is the inability to update configuration, update software, or place and receive calls.

Actions required to mitigate:

1. Upgrade all phones to a minimum of UC Software 4.0.x
2. Replace legacy units with current generation VVX phones – trade-in programs are available
3. Create a custom Private Key Infrastructure (PKI) including your own certificate issuing Root Authority and install this private root authority's public certificate onto your legacy Polycom models so that you may continue to issue your own SHA1 signed certificates.

You can find details on how to install custom CA certificates in the Polycom Administrator Guide.

Note that this Engineering Advisory does not provide details on creating your own PKI and Root Certification Authority.

Polycom Trade-in Programs and Purchasing Incentives

Buy VVX desk phones as trade-ins, receiving rebates of $10-$25 each.
http://connect.polycom.com/content/polycom/ppn/home/resources/sales-tools/promotions.html

UC Software Versions and Their Supported SHA256 Signed Certificates

Any UC Software version not listed below does not include by default a trusted Root Certificate signed with SHA256.

UCS 4.0.7

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Entrust Root Certification Authority - G2	2048 bit	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT
GeoTrust Primary Certification Authority - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT

Certificate CN	*RSA Public Key*	*Start*	*End*
Thawte Primary Root CA - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 4.0.8

Includes the above 4.0.7 certificates as well as the addition of:

Certificate CN	*RSA Public Key*	*Start*	*End*
VeriSign Universal Root Certification Authority	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 4.1.0, 4.1.1, and 4.1.2

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT

UCS 4.1.0 – 4.1.6

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT

UCS 4.1.7, 4.1.8

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Entrust Root Certification Authority - G2	2048 bit	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT
GeoTrust Primary Certification Authority - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Thawte Primary Root CA - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 4.1.9

Includes the above 4.1.8 certificates as well as the addition of:

Certificate CN	*RSA Public Key*	*Start*	*End*
VeriSign Universal Root Certification Authority	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 5.0.0, 5.0.1

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT

UCS 5.1.0 - 5.1.3

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Entrust Root Certification Authority - G2	2048 bit	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT
GeoTrust Primary Certification Authority - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Thawte Primary Root CA - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 5.2 – 5.2.1

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Entrust Root Certification Authority - G2	2048 bit	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT
GeoTrust Primary Certification Authority - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Thawte Primary Root CA - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT

UCS 5.2.2

Includes the above 5.2 certificates as well as the addition of:

Certificate CN	*RSA Public Key*	*Start*	*End*
VeriSign Universal Root Certification Authority	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
DigiCert Assured ID Root G2	2048 bit	Aug 1 12:00:00 2013 GMT	Jan 15 12:00:00 2038 GMT
DigiCert Global Root G2	2048 bit	Aug 1 12:00:00 2013 GMT	Jan 15 12:00:00 2038 GMT

UCS 5.3

Certificate CN	*RSA Public Key*	*Start*	*End*
Go Daddy Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Entrust Root Certification Authority - G2	2048 bit	Jul 7 17:25:54 2009 GMT	Dec 7 17:55:54 2030 GMT
GeoTrust Primary Certification Authority - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	2048 bit	Sep 1 00:00:00 2009 GMT	Dec 31 23:59:59 2037 GMT
Thawte Primary Root CA - G3	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
VeriSign Universal Root Certification Authority	2048 bit	Apr 2 00:00:00 2008 GMT	Dec 1 23:59:59 2037 GMT
DigiCert Assured ID Root G2	2048 bit	Aug 1 12:00:00 2013 GMT	Jan 15 12:00:00 2038 GMT
DigiCert Global Root G2	2048 bit	Aug 1 12:00:00 2013 GMT	Jan 15 12:00:00 2038 GMT

6001 America Center Drive

San Jose, CA 95002

USA

Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.