Security Advisory Report - OBSO-1701-01

SHA-1 certificates: depreciation in 2017

Creation Date: 2017-01-03
Last Update: 2017-01-03

Summary

In the first quarter of 2017, the major internet web browser applications will be introducing some changes that could potentially affect how users access our OpenScape and HiPath based solutions.

If the OpenScape or HiPath solution makes use of secure connections for signaling, administrative or end-user service delivery then certificates would have been applied to one or more of the solution elements.
The major browser vendors have decided to start warning end users that accessing sites whose certificates were constructed using a particular algorithm (SHA-1) could be vulnerable.

If certificates of this type are present in the solution then end users or potentially operators may see a change in behavior or be blocked from reaching these sites.

Vulnerability Details

When establishing a browser based session to remote systems, certificates are used to create a trusted relationship between the endpoints.
Certificates have been used for many years and over time the algorithms used to create them have matured to keep pace with the ability of technology to decipher them.
One of the more popular algorithms currently used to sign certificates is SHA-2, and preceding this, SHA-1 was used widely.

The industry is attempting to phase out SHA-1 based certificates and in Q1, 2017 the three main web browsers (Internet Explorer, Chrome and Firefox) will introduce functionality to their applications that will start impairing access to certificates that use SHA-1.
Initially, they will ask the user to acknowledge that the site may not be secure and it is very possible that at some time the browsers will raise the bar further and block access completely.

Historically, SHA-1 has been used extensively within Unify portfolio and while many of our customers have moved to SHA-2 over the past few years, we know that SHA-1 based certification remain in some customer environments.
To maintain the highest level of overall service delivery we are asking our customers to review their current certificate strategy and determine if any action is required within the OpenScape/HiPath environments.

The SHA1 deprecation will not affect self signed certificates and enterprise root CAs.
Unless any customer has issued a certificate from a public CA, they can continue to use SHA1 certificates short term.

We include the information following as a reminder of the implications that changing browser functionality can have on the OpenScape solution and we request that you track and respond appropriately to any subsequent actions taken by the browser or other third party elements

Microsoft IE
http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx
In February 2017, there will be no impact for roots that are not included in Microsoft Trusted Root Program, such as enterprise or self-signed roots that you have chosen to trust.

Firefox will do the same
https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/
SHA-1 certificates that chain up to a manually-imported root certificate, as specified by the user, will continue to be supported by default

Chrome does the same, via a separate flag that enterprises can enable and provides a final day when this will be removed (Jan. 2019)
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
Starting with Chrome 54 we provide the EnableSha1ForLocalAnchors policy that allows certificates which chain to a locally installed trust anchor to be used after support has otherwise been removed from Chrome

Affected Products

If an element of the solution is configured to use an SHA-1 based certificate, then secure communications to this system is potentially at risk.
The application software version does not affect this.

To determine if that solution element will be at risk, the following should be considered:
- End users or administrators access the solution element over a secured connection established with a web browser, **and**
- The certificate used was signed using the SHA-1 algorithm, **and**
- The certificate was obtained from a public certificate authority (CA).

Secured connections between solution elements (for example, the connection between a UC backend server and a Façade application server) are not affected as neither endpoint utilizes browsers for these connections.

Product that support SHA-2 signed certificated and version of SHA-2 Introduction

OpenScape Voice V8 R1 PS39, V9
OpenScape 4000 V7, V8
OpenScape DLS V7 R3
OpenScape Business/ Office Nov 2015 with RQ39682/ I5133
OpenScape UC, CMP All versions
OpenScape Xpressions V7 R0, R1
OpenScape Contact Center V8 R2, V9
OpenScape Contact Center Extensions V3 R1
OpenScape Fault Management V8, V9
OpenScape ACC V2, V1 R2
OpenScape FM V8, V9
OS SBC V7 R1, V8, V9
OS Branch V7 R1, V8, V9
OS Phones
  OS CP200/400/600 SIP, CP200 HFA
  OS V2 R2.30 (SIP) and later
  OS V2 R0.70 (HFA) and later
  OS V2 R0.70 (TDM) and later
OpenScape Desktop Client/Fusion all versions
OScAR-Pro V4 R1 and later

Recommended Actions

For a solution that is at risk, an updated certificate is required to address the underlying concern and allow the browsers to allow direct access to the sites.
The preferred solution is to obtain and distribute a SHA-2 based certificate.

Support for SHA-2 is available across the OpenScape solution.
As a short-term workaround the existing SHA-1 based certificate can be replaced with a new SHA-1 or better SHA-2 self-signed certificate.
The browser vendors claim that they will not enforce any new rules for secure session to sites using self-signed certificates.

References

https://blogs.windows.com/msedgedev/2016/04/29/sha1-deprecation-roadmap/#VJWVOqqZCiuxEAsd.97

https://blog.qualys.com/ssllabs/2014/09/09/sha1-deprecation-what-you-need-to-know

Revision History

2017-01-03 Initial release planned

Advisory ID: OBSO-1701-01 (a=159), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com