EXECUTIVE BRIEF

Impending SHA-1 Deadlines Can Impact Your Business

The cyber security industry, audit organizations, technical experts, browser manufacturers, Microsoft, and standards organizations agree: SHA-1 signed certificates need to be replaced. Starting as early as June 2016, active SHA-1 certificates can have serious impact on your business for both internal PKI and external brand reputation. This includes:

IMPACT TO BUSINESS	LOSS OF PRODUCTIVITY (INTERNAL IMPACT)	LOSS OF BUSINESS (EXTERNAL IMPACT)
Unexpected service interruptions and business outages	✓	✓
Failed system-to-system communication where SHA-2 is only accepted but systems are still using SHA-1	✓	✓
Application failure on Windows 10 systems after January 1, 2017	✓	
Collision attacks to steal the private keys which are instrumental in man-in-the-middle attacks		✓
Lack of standards compliance		✓
Negative impact on your brand		✓

23,000+
Keys and Certificates
Are in today's average enterprise[1]

24% Still Use SHA-1
Out of the world's top 143,0000 websites[2]

1.5 Million
SHA-1 Certificates
Set to expire beyond January 1, 2017[3]

200+ Certificates
Become unwieldy to track, according to Gartner[4]

54% of Organizations
Are unaware of how many keys and certificates are in use[1]

$15 Million
Is the total possible impact per outage[1]

Weak SHA-1 Algorithm Puts Your Security at Risk

From a security perspective, a SHA-1 collision attack can create a forged certificate which allows a cybercriminal to impersonate your organization for an investment as low as $75,000. When an attacker creates a forged certificate with the same hash value (or fingerprint) as the original, the attacker can perform man-in-the-middle attacks on TLS connections and steal your data.

The consequences of this type of attack were clearly illustrated in the state-sponsored, Flame malware. Flame took advantage of a weak MD-5 hashing algorithm via a collision attack. SHA-1 certificates also suffer from a weak hashing algorithm and this same weakness can be exploited in a similar fashion.

Currently all browsers provide a warning if a SHA-1 certificate is present and if it's expired. By ignoring the browser warnings your employees are being trained to ignore security warnings and their larger consequences. This type of bad security conditioning could result in employees ignoring a certificate warning for a fraudulent certificate that is being used on a spoofed website as part of a phishing attack.

Operational Risks Can Impact Your Bottom Line

Businesses simply can't afford interruptions, especially outages created by preventable IT issues. While SHA-1 browser warnings will be elevated in June 2016, by January 1, 2017, you'll see service interruptions as browsers and operating systems, like Windows 10, block the connection because they no longer accept SHA-1 signed certificate connections.

In January, if your systems using SHA-1 attempt to establish secure connections to systems that only accept SHA-2, your connection will be refused. A good example of the impact was illustrated in January 2016, when Mozilla decided to proactively block SHA-1 connections to improve security. Chaos ensued when security gateway solutions—that still used SHA-1 certificates to perform a TLS inspection—were blocked by the Firefox browser.

Standards Bodies Support Migration

Regulating bodies like NIST have already issued guidance that SHA-1 has been deprecated since December 31, 2013 because it is susceptible to collision attacks. The CA/Browser Forum also provides guidelines that the issuance of certificates from CAs should not have an expiry date greater than January 1, 2017.

ABOUT VENAFI

Venafi is the leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage, secure, and protect cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility.

[1] Ponemon Institute. 2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point. 2015.

[2] SSL Pulse Project: https://www.trustworthyinternet.org/ssl-pulse/

[3] Venafi research

[4] D'Hoinne, Jeremy and Hils, Adam. Gartner. Security Leaders Must Address Threats from Rising SSL Traffic. Gartner RAS Core Research Note G00258176. December 9, 2013.

SHA-1 Applications Are Also at Risk

In addition to browsers, applications that use SHA-1 will also leave you exposed. Microsoft Windows systems (with the applied patch) will not trust files that are signed with code-signing certificates timestamped after January 1, 2016. This will result in application failure. Systems that do not have the patch applied and still trust SHA-1 signed code, will be at significant risk of another Flame-type attack. It's important that you plan to replace vulnerable SHA-1 certificates early, as many browser manufacturers are still considering accelerating the January 2017 deadline.

Cybercriminals have already broken SHA-1 because it's so inexpensive to perform the attack. But the operational costs to your business may not be minimal. For example, IP phones need to be upgraded at a cost to the business. If they are not, TLS sessions cannot be established between systems that only support SHA-1 and systems that only support SHA-2, which means the phones won't work.

Not only is it time to have a solid migration plan, but it's also time to budget for equipment changes to avoid business interruption.

Negative Impact on Your Brand

Customers must have confidence in the security and privacy of transactions before they are willing to do business with your organization. You never want to have a visitor to your website be told your company is NOT trustworthy.

When triggered, SHA-1 bowser security warnings say the following:

- "This site uses weak security configuration, (SHA-1 signatures), so your connection may not be private."
- "Your connection uses an obsolete cipher suite"
- "These resources can be viewed by others while in transit, and can be modified by attacker to change the look of the page."

This kind of messaging conveys risk, creates a poor user experience and reduces trust in your brand. It can be seen by all users who engage with your website—by customers, investors, board members—undermining your brand reputation and causing trust and integrity issues at the highest levels of your organization.

Venafi Can Accelerate Your Migration

Venafi is uniquely capable of helping you and your organization accelerate your SHA-1 migration by providing the following:

- Rapidly discover all of your SHA-1 certificates across your networks, cloud instances, CA's and trust stores
- Fully automate the migration, revocation, issuance, replacement & installation of SHA-1 certificates regardless of which Certificate Authority they were generated from
- Implement robust, policy-enforced controls and workflows so that SHA-1 certificates do not re-appear within your infrastructure
- Provide complete visibility and validation into the migration process via dashboards and reports
- Lower your costs to automate and perform all of these tasks

For more information regarding the SHA-1 migration:
Read the SHA-1 Migration Guide