Do You Know If You Still Have SHA-1 Certificates?

Over 20% of websites still use vulnerable SHA-1 certificates

Microsoft EDGE and IE 11 are now blocking SHA-1 certificates and all major browsers have been flagging SHA-1 with security warnings for months. Yet, despite these stringent measures, many websites still use the deprecated SHA-1 algorithm. Venafi Labs recently discovered that, in a survey of over 33 million publicly visible IPv4 websites, 21% still use the exploitable SHA-1 hashing algorithm. Does yours?

Why it's increasingly urgent to find and replace all SHA-1 certificates

SHA-1 has been considered an insecure cryptographic hash algorithm for years.[1] Its vulnerability is nothing new. But what's driving the current sense of urgency? SHA-1 has now been proven to be easy and affordable to exploit. Research recently demonstrated that SHA-1 can be exploited for as little as $75,000 using Amazon Web Services (AWS).[2] As a result, attackers can easily create forged certificates that deliver the same access as an original certificate. These forged certificates can be used to compromise machine identities, which are established by certificates—similar to how usernames and passwords authenticate people. Forged certificates allow attackers unauthorized access to control machine-to-machine communications. Attackers can also use vulnerable certificates to perform a multitude of nefarious activities, such as man-in-the-middle (MITM) attacks or sign malicious code so that it appears to come from a trusted source.

What you need to do (and why it's harder than you might think)

To protect your machine identities against the malicious exploit of SHA-1 certificates, you will need to find and replace all outstanding SHA-1 certificates. Yet most businesses do not have the visibility they need to locate and replace all of the certificates which control machine identities, let alone determine which algorithm they use. This is especially challenging for internal certificates. They are harder to discover, manage and migrate—mainly because they are spread throughout the enterprise and owned by different organizational units. In addition, you'll need to discover which legacy systems aren't compatible with SHA-2 algorithms so you can evaluate appropriate remediation options.

It doesn't have to be so hard

Don't have the time or budget to engage a consulting firm in a lengthy project? There's an easier way to find and replace all outstanding SHA-1 certificates. Using an automated key and certificate management system, you can quickly inventory known and unknown certificates throughout your enterprise. This visibility allows you to quickly see which keys and certificates are vulnerable and still need to be migrated to SHA-2. Plus, you will be able to prioritize and automate the replacement of SHA-1 certificates. Automation helps you avoid the delays and errors of manual processes that can cause outages in certificate-dependent systems as well as other security and availability issues.

1. Schneier, Bruce. Schneier on Security Blog. Cryptanalysis of MD5 and SHA: Time for a New Standard. August 19, 2004.
2. Kovacs, Eduard. SecurityWeek. New Collision Attack Lowers Cost of Breaking SHA1. October 8, 2015.

How Venafi can help

Venafi equips you with a comprehensive, objective understanding of your SHA-1 status. This independent view is much more effective than relying solely on your CA, which gives you only a partial picture of the certificates in use across your enterprise. Venafi also helps you to prioritize your certificates that are using SHA-1 so your team can effectively triage the replacement of certificates and start with those most vulnerable to exploitation. By eradicating any remaining SHA-1 certificates, you'll protect the reliability and availability of critical services. Plus, in less time than you'd anticipate, you'll improve security and reduce compliance risks so you can better protect your machine identities.

Venafi can help your organization complete its SHA-1 migration

- Rapidly discover all SHA-1 certificates across networks, cloud instances and CAs
- Fully automate the migration of SHA-1 certificates, regardless of CA
- Prevent SHA-1 certificates from reappearing within your infrastructure
- Validate your migration process for compliance audits
- Strengthen key and certificate management across the board

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com