



**Subscribe to Infosecurity Magazine**  
Strategy - Insight - Technology

[Sign Up](#) [Log In](#)

Latest

[Pindron Raises \\$75 Million for Voice-Printing Tech](#)

[News](#) [Topics](#) [Features](#) [Webinars](#) [White Papers](#) [Events & Conferences](#) [Directory](#)

INFOSECURITY MAGAZINE HOME » NEWS » BUSINESSES USING MILLIONS OF FLAWED CERTIFICATES

20 OCT 2015 NEWS

# Businesses Using Millions of Flawed Certificates



Tara Seals US/North America News Reporter, Infosecurity Magazine

[Email Tara](#)

Many big businesses, including firms like Deloitte, are still using SHA-1 certificates, despite the fact that SHA-1 is known to be ineffective.

In fact, 120,000 SHA-1 certificates were issued this year, according to research from Netcraft.

Nearly a million SSL certificates found in Netcraft's October SSL Survey were signed with the potentially vulnerable SHA-1 hashing algorithm, and some certificate authorities are continuing to issue more.

The latest research, dubbed the **SHAppening**, projects that a full SHA-1 collision could be found within 49-78 days on a 512-GPU cluster. Renting the equivalent processing time on Amazon's EC2 cloud computing service would cost only \$75,000 to \$120,000, Netcraft said, "which is an order of magnitude less than earlier estimates."

The researchers point out that this represents an important alarm signal, and that the industry's plans to move away from SHA-1 by 2017 might not be fast enough.

It's now feasible for a well-funded attacker to impersonate an SSL site that uses a publicly trusted SHA-1 certificate. Worse still, while browsers still accept SHA-1 signatures, SSL sites remain at risk even after migrating to SHA-2: if an attacker were to compromise an intermediate CA certificate signed with SHA-1, he could generate valid certificates for arbitrary domains.

The SHA-2 and SHA-3 family of cryptographic hash algorithms are now the only ones approved by the National Institute of Standards and Technology (NIST) for digital signature generation. Although the SHA-2 family includes SHA-224, only the stronger SHA-256, SHA-384 and SHA-512 algorithms are allowed by the CA/Browser Forum's Baseline Requirements for the issuance and management of publicly-trusted certificates.

Tod Beardsley, principal security research manager at **Rapid7**, said that certificate authorities

## Why Not Watch?



2 APR 2015  
Browsers, Certificates and Trust: What's Changing and What You Need to Know



21 JAN 2016  
Don't Be Blind On Visibility



need to take the lead in eliminating the use of SHA-1.

“Certificate authorities need to step up, sooner rather than later, to replace obsolete SHA-1 certificates with the more modern and more secure SHA-2 certificates,” he said via email. “Time and technology marches on, and it’s not as if the current population of SHA-1 certs will get any harder to attack with common, off-the-shelf equipment.”

There are positive steps happening: Google **announced plans** last year to retire SHA-1 in its browser;

SHA-1’s weaknesses in collisions **have been known publicly** since at least 2005, as reported by Bruce Schneier.

He added that it’s the comfort of the familiar that appears to be the biggest obstacle in moving on from SHA-1.

“Today, there is no practical reason to continue issuing SHA-1 certs, except for the most common reason that keeps all old technology alive: institutional inertia,” he said. “This is the same force that keeps us in magstripe card readers, cleartext Internet protocols, and unchangeable, secret-yet-not-secret social security numbers, and any number of other older technologies being thrust onto a global and increasingly hostile internet.”

### Recommended for you



Password Cracker Cracks 55 Charac...  
www.infosecurity-mag...



What Can a Hacker Do with S...  
www.infosecurity-mag...



Scariest Search Engine on the Int...  
www.infosecurity-mag...



NIST issues guidelines for pu...  
www.infosecurity-mag...

AddThis

0 Comments

Infosecurity Magazine

Login

Recommend

Share

Sort by Best



Start the discussion...

Be the first to comment.

#### ALSO ON INFOSECURITY MAGAZINE

##### Average Cost of a Spear Phishing Incident: \$1.6Mn

1 comment • 19 days ago

Avatar**Ross Morley** — Data thieves - whether external or internal - will always find a way. My service protects your data ...

##### Cyber-Bonanza: 80% of Android Users Have Outdated Smartphones

#### Our website uses cookies

Cookies enable us to provide the best experience possible and help us understand how visitors use our website. By browsing Infosecurity Magazine, you agree to our use of cookies.

Okay, I understand

Learn more

#### WHAT'S THIS?

##### OpenSSL to Patch a High-Severity Flaw

1 comment • 7 days ago

Avatar**ghana** — Good to know about the upcoming updates that fixes high and low severity issues.

##### Religious Apps Put on the High Risk List by Proofpoint

1 comment • 2 months ago

Avatar**Matt** — Is there a link to the published list of malware apps? Not much help if we don't know which ones to uninstall or ...



9 APR 2015  
Crunch Time for Securing Big Data



7 JAN 2016  
The 'Dark' Web Inside Your Enterprise – Shining a Light on the Hazards of Encrypted Traffic

## Related to This Story

Dell PCs Ship Preloaded with Flawed Certificates

Web Owners Urged to Upgrade From Insecure SHA-1 Algorithm

Online Daters Targeted by Massive Phishing Campaign

Most Security Depts Blindly Trust Certificates and Keys

Multiple Digital Certificate Attacks Affect 100% of UK Businesses

## What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

- 1 FEB 2016 NEWS  
**Silver Lining for IT Professionals**
- 29 JAN 2016 NEWS  
**HSBC Banking Customers Vent Anger After DDoS Scuppers Service**
- 1 FEB 2016 NEWS  
**Ransomware Shuts Down Lincolnshire Council IT Systems for Days**
- 1 FEB 2016 NEWS  
**US Security Firm Norse Sacks CEO – Report**
- 30 JAN 2015 NEWS  
**Adult Site Xhamster Hit by 'Huge' Malvertising Attack**
- 29 JAN 2016 NEWS  
**Exclusive: School Websites Contain Pornographic and Gambling Links**