LOLLOL - FOTOLIA

MD5 vulnerability renews calls for faster SHA-256 transition

by
Michael Heller
Senior Reporter

Published: 07 Jan 2016

Researchers have found a way to exploit an MD5 vulnerability in a new way to put users at risk, and experts say this is all the more reason to move faster in transitioning to SHA-256.

THIS ARTICLE COVERS
Web Browser Security »

+ Show More

The MD5 hash function has had a rocky history right from the start and researchers are still finding new ways to exploit its vulnerabilities even as many companies are actively transitioning away from the technology.

In a research paper published this week, authors from French research institute INRIA identified a new class of transcript collision attacks affecting "mainstream" key exchange protocols like TLS, IKE, and SSH. Such attacks were thought to be too resource intensive to be performed reliably, but the researchers found that an attacker would be able to successfully impersonate an end user in about one hour.

According to Michael Taylor, applications and product development lead for Rook Security, the attacks work by generating a collision, or a

scenario where two different inputs into an encryption protocol algorithm yield the same result.

"If a user and a legitimate site are both using a protocol like TLSv1.1 that relies on SHA-1 and MD5 and the user can be tricked into visiting a compromised site as well as a legitimate site, then the compromised one may be able to impersonate the user to the legitimate site. Both the authentic site and the end user must be using one of the weak encryption protocols," Taylor said. "MD5 was intended to have very few instances of these collision scenarios, but because of how it is implemented within these protocols, the attacker must calculate a lower number of cryptographic hashes before finding a collision. This allows the attacker the ability to then communicate to the legitimate server as though he or she is the end user."

The researchers call attacks like this "SLOTH" or Security Losses from Obsolete and Truncated Transcript Hashes, and note this is "a not-so-subtle reference to laziness in the protocol design community with regard to removing legacy cryptographic constructions."

Wes Widner, director of threat intelligence at Norse, said MD5 vulnerabilities were found very quickly after the hash function was first introduced.

"MD5 was designed in 1991 as a secure replacement for MD4. In 1996 a fatal flaw was found in MD5 and subsequent flaws were found in 2004, 2005, 2006, 2007 and 2008," Widner said. "As of 2010, the CMU Software Engineering Institute considered MD5 'cryptographically broken and unsuitable for further use'. Most US government applications now require SHA-2hashes."

Taylor said MD5 is still one of the most common hash algorithms used today in spite of the risks it poses.

"The reluctance to move away from MD5 is most likely due to people being willing to accept the collision risk for the vast majority of file signing scenarios where there is not an'adversary'attempting to manipulate the data, but the end user wants to verify that their file was transferred without corruption."

While experts agree that MD5 should be left behind in favor of SHA-256, and companies have been pushing to abandon SHA-1, Widner said there are still hurdles to be jumped, and the final move may not happen until SHA-1 is broken in the same way this research breaks MD5.

"The long and short of it is that generating lots of SHA-256 hashes takes a lot of time and energy. Both of those are enemies of large scale computing so people tend to avoid them as much as possible," Widner said. "The second reason SHA-256 hasn't been adopted more widely, specifically in cryptographic systems: SHA-1 hasn't been broken yet. Vulnerabilities have been discovered but a hash collision hasn't been achieved yet. I would argue that being able to generate a hash collision with MD5 is what motivated people to stop using it in secure systems. SHA-1 will suffer the same fate if/when a hash collision is demonstrated with it."

Michael Cobb, CISSP-ISSAP and renowned security author, said there needs to be better cooperation to move past vulnerable protocols.

"The Internet will always be plagued by weak encryption algorithms if newer versions of protocols such as TLS have to be backwards compatible to support older versions," Cobb said. "Until the industry can agree on deadline dates after which xx protocol will no longer be supported, enterprises will always drag their feet and delay upgrading code that may be insecure but runs mission critical processes."

Next Steps

Learn if it is time to make the move to the SHA-2 algorithm.

Learn about the future of SSL and enterprise application security.

Experts believe SHA-1 could be undermined soon.

Dig Deeper on Web Browser Security

ALL NEWS GET STARTED EVALUATE MANAGE PROBLEM SOLVE

- How client-side injection malware hijacks e-commerce traffic
- Should the RC4 cipher still be used in enterprises?
- Symantec asks browser makers to distrust one of its root certificates
- Should enterprises use an open certificate authority?

Load More

0 comments Oldest ▾

Share your comment

Send me notifications when other members comment.

Register or Login

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and

Breaking down the Amazon EC2 key recovery attack

A research paper demonstrating a key recovery attack on Amazon Web Services' EC2 illustrates the risks of colocation and ...

Why BYOK is so attractive despite its risks

BYOK encryption services are a new trend among enterprises, despite all the challenges and risks that accompany them. Expert Dave...