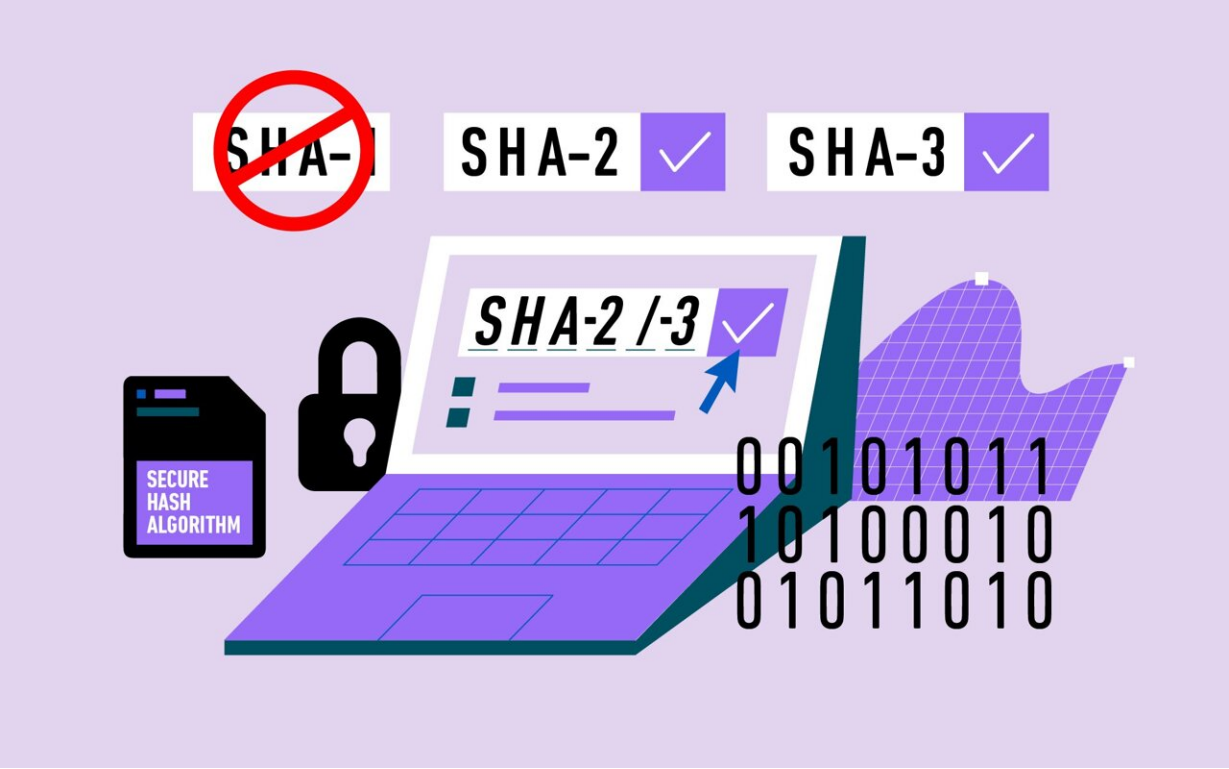
NIST retires SHA-1 cryptographic algorithm due to vulnerabilities

December 16 2022



NIST recommends that anyone relying on SHA-1 for security switch to using the more secure SHA-2 and SHA-3 groups of algorithms. Credit: B. Hayes/NIST

The SHA-1 algorithm, one of the first widely used methods of protecting electronic information, has reached the end of its useful life, according to security experts at the National Institute of Standards and Technology

(NIST). The agency is now recommending that IT professionals replace SHA-1, in the limited situations where it is still used, with newer algorithms that are more secure.

SHA-1, whose initials stand for "secure hash algorithm," has been in use since 1995 as part of the Federal Information Processing Standard (FIPS) 180-1. It is a slightly modified version of SHA, the first hash function the federal government standardized for widespread use in 1993. As today's increasingly powerful computers are able to attack the algorithm, NIST is announcing that SHA-1 should be phased out by Dec. 31, 2030, in favor of the more secure SHA-2 and SHA-3 groups of algorithms.

"We recommend that anyone relying on SHA-1 for security migrate to SHA-2 or SHA-3 as soon as possible," said NIST computer scientist Chris Celi.

SHA-1 has served as a building block for many security applications, such as validating websites—so that when you load a webpage, you can trust that its purported source is genuine. It secures information by performing a complex math operation on the characters of a message, producing a short string of characters called a hash. It is impossible to reconstruct the original message from the hash alone, but knowing the hash provides an easy way for a recipient to check whether the original message has been compromised, as even a slight change to the message alters the resulting hash dramatically.

Today's more powerful computers can create fraudulent messages that result in the same hash as the original, potentially compromising the authentic message. These "collision" attacks have been used to undermine SHA-1 in recent years. NIST has announced previously that federal agencies should stop using SHA-1 in situations where collision attacks are a critical threat, such as for the creation of digital signatures.

As attacks on SHA-1 in other applications have become increasingly severe, NIST will stop using SHA-1 in its last remaining specified protocols by Dec. 31, 2030. By that date, NIST plans to:

- Publish FIPS 180-5 (a revision of FIPS 180) to remove the SHA-1 specification.
- Revise SP 800-131A and other affected NIST publications to reflect the planned withdrawal of SHA-1.
- Create and publish a transition strategy for validating cryptographic modules and algorithms.

The last item refers to NIST's Cryptographic Module Validation Program (CMVP), which assesses whether modules—the building blocks that form a functional encryption system—work effectively. All cryptographic modules used in federal encryption must be validated every five years, so SHA-1's status change will affect companies that develop modules.

"Modules that still use SHA-1 after 2030 will not be permitted for purchase by the federal government," Celi said. "Companies have eight years to submit updated modules that no longer use SHA-1. Because there is often a backlog of submissions before a deadline, we recommend that developers submit their updated modules well in advance, so that CMVP has time to respond."

More information: Questions about the transition can be sent to sha-1-transition@nist.gov. More information is available at the NIST Computer Security Resource Center transition page.

Provided by National Institute of Standards and Technology