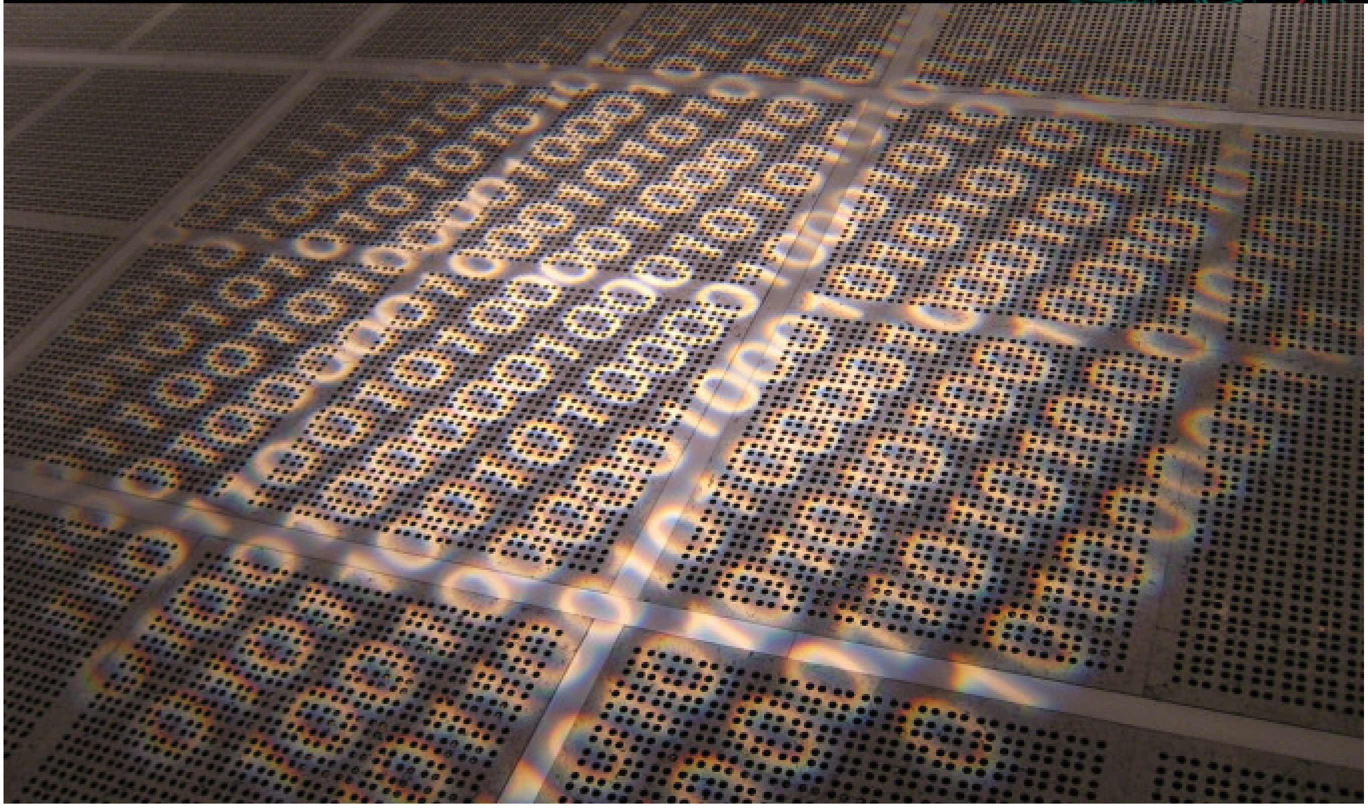

Microsoft Warns Customers Away From SHA-1 & RC4

by Dennis Fisher November 12, 2013 , 4:07 pm

The RC4 and SHA-1 algorithms have taken a lot of hits in recent years, with new attacks popping up on a regular basis. Many security experts and cryptographers have been recommending that vendors begin phasing the two out, and Microsoft on Tuesday said that is now recommending to developers that they deprecate RC4 and stop using the SHA-1 hash algorithm.

RC4 is among the older stream cipher suites in use today, and there have been a number of practical attacks against it, including plaintext-recovery attacks. The improvements in computing power have made many of these attacks more feasible for attackers, and so Microsoft is telling developers to drop RC4 from their applications.

Related Posts

Surveillance Backdoors 'Contribute to Insecurity', Report Says

November 13, 2013 , 10:28 am

Microsoft November Patch Updates Fix One of Two Known Zero Days

November 12, 2013 , 3:51 pm

Selfish Miners Could Exploit P2P Nature of Bitcoin Network

November 12, 2013 , 10:34 am

“In light of recent research into practical attacks on biases in the RC4 stream cipher, Microsoft is recommending that customers enable TLS1.2 in their services and take steps to retire and deprecate RC4 as used in their TLS implementations. Microsoft recommends TLS1.2 with AES-GCM as a more secure alternative which will provide similar performance,” Microsoft’s William Peteroy said in a blog post.

“One of the first steps in evaluating the customer impact of new security research and understanding the risks involved has to do with evaluating the state of public and customer environments. Using a sample size of five million sites, we found that 58% of sites do not use RC4, while approximately 43% do. Of the 43% that utilize RC4, only 3.9% require its use. Therefore disabling RC4 by default has the potential to decrease the use of RC4 by over almost forty percent.”

The software company also is recommending that certificate authorities and others stop using the SHA-1 algorithm. Microsoft cited the existence of known collision attacks against SHA-1 as the main reason for advising against its use. Also, after January 2016, Microsoft developers can no longer use SHA-1 in code-signing or developer certificates.