Google Security Blog

The latest news and insights from Google on security and safety on the Internet

An update on SHA-1 certificates in Chrome

December 18, 2015

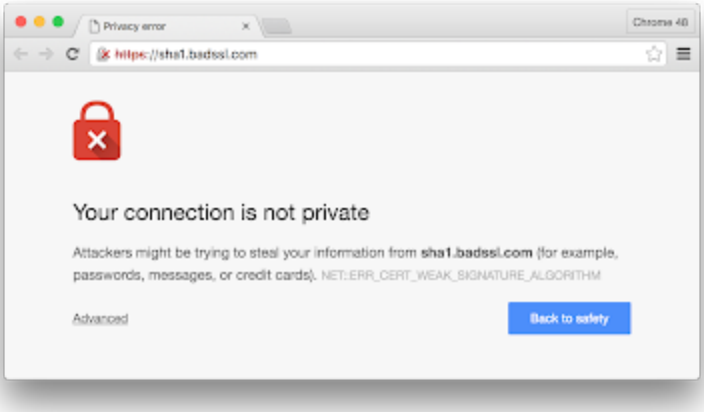
Posted by Lucas Garron, Chrome security and David Benjamin, Chrome networking

As announced last September and supported by further recent research, Google Chrome does not treat SHA-1 certificates as secure anymore, and will completely stop supporting them over the next year. Chrome will discontinue support in two steps: first, blocking new SHA-1 certificates; and second, blocking all SHA-1 certificates.

Step 1: Blocking new SHA-1 certificates

Starting in early 2016 with Chrome version 48, Chrome will display a certificate error if it encounters a site with a leaf certificate that:

1. is signed with a SHA-1-based signature
2. is issued on or after January 1, 2016
3. chains to a public CA



We are hopeful that no one will encounter this error, since public CAs must stop issuing SHA-1 certificates in 2016 per the Baseline Requirements for SSL.

In addition, a later version of Chrome in 2016 may extend these criteria in order to help guard against SHA-1 collision attacks on older devices, by displaying a certificate error for sites with certificate chains that:

1. contain an intermediate or leaf certificate signed with a SHA-1-based signature
2. contain an intermediate or leaf certificate issued on or after January 1, 2016
3. chain to a public CA

(Note that the first two criteria can match different certificates.)

Note that sites using new SHA-1 certificates that chain to local trust anchors (rather than public CAs) will continue to work without a certificate error. However, they will still be subject to the UI downgrade specified in our original announcement.

Step 2: Blocking all SHA-1 certificates

Starting January 1, 2017 at the latest, Chrome will completely stop supporting SHA-1 certificates. At this point, sites that have a SHA-1-based signature as part of the certificate chain (not including the self-signature on the root certificate) will trigger a fatal network error. This includes certificate chains that end in a local trust anchor as well as those that end at a public CA.

In line with Microsoft Edge and Mozilla Firefox, the target date for this step is January 1, 2017, but we are considering moving it earlier to July 1, 2016 in light of ongoing research. We therefore urge sites to replace any remaining SHA-1 certificates as soon as possible.

Note that Chrome uses the certificate trust settings of the host OS where possible, and that an update such as Microsoft's planned change will cause a fatal network error in Chrome, regardless of Chrome's intended target date.

Keeping your site safe and compatible

As individual TLS features are found to be too weak, browsers need to drop support for those features to keep users safe. Unfortunately, SHA-1 certificates are not the only feature that browsers will remove in the near future.

As we announced on our security-dev mailing list, Chrome 48 will also stop supporting RC4 cipher suites for TLS connections. This aligns with timelines for Microsoft Edge and Mozilla Firefox.

For security and interoperability in the face of upcoming browser changes, site operators should ensure that their servers use SHA-2 certificates, support non-RC4 cipher suites, and follow TLS best practices. In particular, we recommend that most sites support TLS 1.2 and prioritize the ECDHE_RSA_WITH_AES_128_GCM

cipher suite. We also encourage site operators to use tools like the SSL Labs server test and Mozilla's SSL Configuration Generator.

No comments :

Post a Comment