Google Security Blog

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

Chrome's Plan to Distrust Symantec Certificates

September 11, 2017

Posted by Devon O'Brien, Ryan Sleevi, Andrew Whalley, Chrome Security

This post is a broader announcement of plans already finalized on the blink-dev mailing list.

At the end of July, the Chrome team and the PKI community converged upon a plan to reduce, and ultimately remove, trust in Symantec's infrastructure in order to uphold users' security and privacy when browsing the web. This plan, arrived at after significant debate on the blink-dev forum, would allow reasonable time for a transition to new, independently-operated Managed Partner Infrastructure while Symantec modernizes and redesigns its infrastructure to adhere to industry standards. This post reiterates this plan and includes a timeline detailing when site operators may need to obtain new certificates.

On January 19, 2017, a public posting to the mozilla.dev.security.policy newsgroup drew attention to a series of questionable website authentication certificates issued by Symantec Corporation's PKI. Symantec's PKI business, which operates a series of Certificate Authorities under various brand names, including Thawte, VeriSign, Equifax, GeoTrust, and RapidSSL, had issued numerous certificates that did not comply with the industry-developed CA/Browser Forum Baseline Requirements. During the subsequent investigation, it was revealed that Symantec had entrusted

several organizations with the ability to issue certificates without the appropriate or necessary oversight, and had been aware of security deficiencies at these organizations for some time.

This incident, while distinct from a previous incident in 2015, was part of a continuing pattern of issues over the past several years that has caused the Chrome team to lose confidence in the trustworthiness of Symantec's infrastructure, and as a result, the certificates that have been or will be issued from it.

After our agreed-upon proposal was circulated, Symantec announced the selection of DigiCert to run this independently-operated Managed Partner Infrastructure, as well as their intention to sell their PKI business to DigiCert in lieu of building a new trusted infrastructure. This post outlines the timeline for that transition and the steps that existing Symantec customers should take to minimize disruption to their users.

Information For Site Operators

Starting with Chrome 66, Chrome will remove trust in Symantec-issued certificates issued prior to June 1, 2016. Chrome 66 is currently scheduled to be released to Chrome Beta users on March 15, 2018 and to Chrome Stable users around April 17, 2018.

If you are a site operator with a certificate issued by a Symantec CA prior to June 1, 2016, then prior to the release of Chrome 66, you will need to replace the existing certificate with a new certificate from any Certificate Authority trusted by Chrome.

Additionally, by December 1, 2017, Symantec will transition issuance and operation of publicly-trusted certificates to DigiCert infrastructure, and certificates issued from the old Symantec infrastructure after this date will not be trusted in Chrome.

Around the week of October 23, 2018, Chrome 70 will be released, which will fully remove trust in Symantec's old infrastructure and all of the certificates it has issued. This will affect any certificate chaining to Symantec roots, except for the small number issued by the independently-operated and audited subordinate CAs previously disclosed to Google.

Site operators that need to obtain certificates from Symantec's existing root and intermediate certificates may do so from the old infrastructure until December 1, 2017, although these certificates will need to be replaced again prior to Chrome 70. Additionally, certificates issued from Symantec's infrastructure will have their validity limited to 13 months. Alternatively, site operators may obtain replacement certificates from any other Certificate Authority currently trusted by Chrome, which are unaffected by this distrust or validity period limit.

Reference Timeline

The following is a timeline of relevant dates associated with this plan, which distills the various requirements and milestones into an actionable set of information for site operators. As always, Chrome release dates can vary by a number of days, but upcoming release dates can be tracked here.

Date	Event
Now through ~March 15, 2018	Site Operators using Symantec-issued TLS server certificates issued before June 1, 2016 should replace these certificates. These certificates can be replaced by any currently trusted CA.
~October 24, 2017	Chrome 62 released to Stable, which will add alerting in DevTools when evaluating certificates that will be affected by the Chrome 66 distrust.
December 1, 2017	According to Symantec, DigiCert's new "Managed Partner Infrastructure" will at this point be capable of full issuance. Any certificates issued by Symantec's old infrastructure after this point will cease working in a future Chrome update. From this date forward, Site Operators can obtain TLS server certificates from the new Managed Partner Infrastructure that will continue to be trusted after Chrome 70 (~October 23, 2018). December 1, 2017 does not mandate any certificate changes, but represents an opportunity for site operators to obtain TLS server certificates that will not be affected by Chrome 70's distrust of the old infrastructure.
~March 15, 2018	Chrome 66 released to beta, which will remove trust in Symantec-issued certificates with a not-before date prior to June 1, 2016. As of this date Site Operators must be using either a Symantec-issued TLS server certificate issued on or after June 1, 2016 or a currently valid certificate issued from any other trusted CA as of Chrome 66. Site Operators that obtained a certificate from Symantec's old infrastructure after June 1, 2016 are unaffected by Chrome 66 but will

	need to obtain a new certificate by the Chrome 70 dates described below.
~April 17, 2018	Chrome 66 released to Stable.
~September 13, 2018	Chrome 70 released to Beta, which will remove trust in the old Symantec-rooted Infrastructure. This will not affect any certificate chaining to the new Managed Partner Infrastructure, which Symantec has said will be operational by December 1, 2017. Only TLS server certificates issued by Symantec's old infrastructure will be affected by this distrust regardless of issuance date.
~October 23, 2018	Chrome 70 released to Stable.

No comments :

Post a Comment

Links to this post

Create a Link