Renegade certificate removed from Windows. Then it returns. Microsoft stays silent.

Getty Images

reader comments

38 with

For three days, system administrators have been troubleshooting errors that have prevented Windows users from running applications such as QuickBooks and Avatax. We now know the cause: an unannounced move or glitch by Microsoft that removed a once-widely used digital certificate in Windows.

The removed credential is known as a root certificate, meaning it anchors the trust of hundreds or thousands of intermediate and individual certificates downstream. The root certificate—with the serial number 18dad19e267de8bb4a2158cdcc6b3b4a and the SHA1 fingerprint 4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5—was no longer trusted in Windows. Because that root was tied to certificates that certify their authenticity and trust, people trying to use or install the app received the error.

Just minutes before this post was scheduled to go live, researchers learned that the certificate had been restored in Windows. It’s unclear how or why that occurred. The certificate immediately below this paragraph shows the

certificate’s status on Thursday. The one below that shows the status as of Friday.

That time Symantec certs were banished from the Internet

Microsoft has yet to respond to a request to explain the errors. It may be that a glitch caused Windows to remove the root certificate. It’s also possible the removal was

intentional, given that it’s one of several that faced an industry-wide blockade following the discovery in 2015 that its parent issuer at the time, Symantec, had improperly issued certificates for google.com, www.google.com, and one other domain. (Symantec sold its certificate authority (CA) businesses to DigiCert in 2017.)

Advertisement

After Google researchers asserted a few weeks later that the number of mis-issued certificates was much higher, Symantec revised the number to 164 certificates for 76 domains and 2,458 certificates for domains that had never been registered. In light of the new information, Google gave Symantec an ultimatim: give a thorough accounting of its ailing certificate authority process or risk having the world’s most popular browser—Chrome—issue scary warnings about Symantec certificates whenever end users visited HTTPS-protected websites that used them.

Some 17 months later, Google made good on the threat after its investigation concluded that for years, Symantec-owned CAs had improperly issued more than 30,000 certificates. The company began preparations to gradually nullify Chrome’s trust in all certificates issued by those CAs, which were sold under brands including Verisign, Thawte, and GeoTrust. Effective immediately at that time, Chrome stopped recognizing any extended validation status of such certificates, and as time went on, the browser revoked more and more of its trust.

Mis-issued certificates represent a critical threat to virtually the entire Internet population; they make it possible for the holders to cryptographically impersonate the affected sites and monitor or tamper with communications sent between visitors and the legitimate servers. In particular, certificates for non-existent domains or domains belonging to parties other than the holder are major violations of the so-called baseline requirements that major browser makers impose on CAs as a condition of being trusted by their software.

Symantec’s transgressions were serious. But given Symantec’s status at the time as one of the biggest issuers of certificates, Google and other stakeholders were in a bind. If Google or other browser makers were to nullify all of the Symantec-issued certificates overnight, it would cause widespread outages. The chaos that would result made the issuer too big to fail. The penalties outlined by Google aimed to minimize such disruptions while exacting a meaningful punishment.

Over the next two years, browser makers and other companies that rely on digital certificates to secure Internet communications gradually phased out trust in the certificates. Most timetables called for a deadline sometime in 2019. For reasons Microsoft has yet to explain, Windows continued to trust the root certificates to sign software.

Advertisement

That trust was finally revoked—or at least suspended—on Tuesday, once again with no explanation or notice. The move sent sys admins scrambling to determine why users were receiving certificate errors when trying to run software such as QuickBooks and AvaTax. Eventually, the CEO of security firm Airlock Digital traced the cause to the unannounced change in Windows.

A Microsoft representative offered to provide comment for this story on the condition the information not be attributed to Microsoft in any way. Ars declined.

It’s likely that Microsoft delayed the revocation of the certificate for app-signing purposes because certificates in apps can’t be updated as easily as they can for websites. With no guidance from the company, people troubleshooting error messages are on their own.

One option for resolving problems is to update affected apps. By now, most apps have likely been updated to use certificates

not related to the ones that have been blocked. By default, Windows has a feature known as automatic root updates turned on. Some users have it turned off for various reasons, many of them legitimate. The above-linked Reddit thread also provides several scripts people can run to rotate out the root certificate.

Update: 10 minutes after Ars declined Microsoft's offer for a not-for-attribution comment, a company representative sent the following statement:

> *The VeriSign Class 3 Public Primary Certification Authority – G5 is distrusted as of 2019 and was set to "NotBefore" in a previous release. This means that certificates issued after the NotBefore date will no longer be trusted; however, certificates issued before the NotBefore date will continue to be trusted. In our August Certificate Trust List update, we changed this setting to Disable as a part of our regular deprecation process which caused some customers with specific configurations to run into issues. On August 24, 2023, we rolled back this change to help remediate these issues.*

https://arstechnica.com/?p=1963549