White Paper

Test Certificates Incident Final Report

Symantec™

10/02/2015
Updated: 10/12/2015

On September 18, 2015, Symantec first discovered and immediately disclosed that a small number of test certificates had been issued inappropriately for several domains, during recent product feature testing by members of our internal QA team. Continuing in that spirit of openness, this is an update on what happened and what has been done since the initial disclosure.

Symantec assessed the risk this activity posed to the Internet community at large. Through a comprehensive internal review, we confirmed this incident was limited only to the issuance of test certificates, which at all times were fully controlled within Symantec and never posed any threat to any user or organization. As soon as we became aware of the incident and understood the risk level, we disclosed this issue. Additionally, we immediately began reaching out to the impacted domain owners to inform them of the situation, share information, and obtain their permission to share more details publicly.

In order to understand the full scope of this kind of activity, including activity prior to Symantec acquiring the Trust Services business, we conducted a full audit of all test certificates. As a result of that exhaustive review, which covered over 100,000 test certificates dating back to 1995, we have identified two (2) additional instances where test certificates were inappropriately issued.

The list of organizations impacted by these test certificates includes Google, Opera, and three (3) other organizations who have not requested or approved disclosure of their domains. Across these organizations, and as a result of our audit, there were a total of twenty three (23) test certificates inappropriately issued as follows: Google (6), Opera (7), and ten (10) other certificates spread over three (3) organizations.

Most importantly, these test certificates never posed a risk to anyone or any organization, as the certificates never left Symantec's secure test labs or the QA test machine, and they were never visible to any end user. Moreover, the test certificates were never used on the QA test machine. Finally, the private keys associated with the test certificates were all destroyed as part of the testing tool that was used to enroll for the test certificates. One of these test certificates with a CN=www.google.com was an Extended Validation (EV) test certificate and was logged to public Certificate Transparency (CT) log servers which is standard practice by default for EV certificates issued by CAs. Logging to a CT server did not in any way make the test certificate usable – it was only detectable by CT monitors.

Despite the minimal risk, and the absence of any threat associated with this issue, we felt that it was important to immediately disclose it. In order to cooperate and work with the domain owners, Symantec has provided the certificate details to those domain owners who have requested them, under the confidentiality agreements with those organizations.

Symantec takes this type of incident extremely seriously and reacted upon notification of the problem by taking the following actions:

1. We identified the pool of certificates that were inappropriately issued for testing, and we ensured they were immediately revoked, even though the certificates never left Symantec's test labs, nor were they ever usable.
2. We launched an audit of all test certificates we've issued – not just for this feature or release, but an exhaustive audit for all test certificates historically since 1995, to ensure we understood the full scope of the issue.
3. We thoroughly analyzed the nature of the test certificates, and more importantly, the nature of how/why they were issued – that informed us of the true risks (e.g. whether the private keys and certificates were exposed – which they were not). This root cause analysis crystalized our remediation steps, and guided us on what actions were necessary to prevent this from occurring again in the future, augmenting the extensive technical controls and procedures already in place.
4. We identified and implemented changes to tools, processes, and personnel to prevent this in the future.

a. Our QA team uses a tool to enroll for certificates in the context of automated testing. This tool can only generate and submit CSRs using public keys for which the corresponding private keys are created, but destroyed in memory and never persisted, and the tool itself is available to a limited number of privileged QA personnel. This tool was misused to enroll for certificates with domains that did not belong to Symantec. We have added technical controls to ensure that neither this tool nor any others can be used to enroll for test certificates for domains that Symantec does not own.
b. When testing features involving Organization or Extended Validation certificates, our authentication team has a specific review and approval process designed for issuance of internal-only Symantec test certificates. The existing policy was explicit that this process should only be used for Symantec-owned domains. That process was not followed in the issuance of these test certificates that included non-Symantec domains. We have updated the test certificate approval process tools and team training to ensure that this process is only applied to the issuance of test certificates for Symantec-owned domains.
c. Finally, we have already enforced accountability given that we take a“no compromise” approach to violations of our policies.

5. We reviewed and updated our threat modeling scenarios – especially focusing on mis-issuance by internal parties. The root cause, in each isolated case, was a violation by specific individuals of established policies governing the issuance of test certificates. This resulted in:
   a. Individuals using test tools inappropriately for enrolling for test certificates for domains that Symantec did not own; and,
   b. Individuals violating existing policies and procedures governing how all test certificates are authenticated.

As the leading certificate authority, a founding member of the CA/Browser Forum, a founding member of the CA Security Council, and one of the largest security software companies in the world, we hold ourselves to very high standards in a constantly evolving security landscape. To that end, we are working towards evolving our own and industry-wide security best practices to deliver a safer digital world for our customers and our partners.

1. We have implemented support for Certification Authority Authorization, enabling customers to explicitly specify from which CAs certificates for their domains may be issued. CAA only works in practice if all CAs support it and if they all explicitly honor customers’ preferences. Symantec has been a champion of CAA and we will be submitting a proposal to make a rule change within the CA/Browser Forum to require all CAs to explicitly support CAA.
2. This incident has demonstrated that logging of certificates to Certificate Transparency log servers, combined with monitoring by domain owners, can be an effective mechanism to detect mis-issued certificates. And while Certificate Transparency is an industry standard, today most CAs that support CT only log public Extended Validation certificates. Symantec does this today and is one of the few organizations that operates its own CT log servers. We have already begun to offer support for logging of Organization Validated certificates, and are planning to offer support for Domain Validated certificates for all customers as well. We are also evaluating making our log servers freely available for all CAs to encourage their support for CT and to increase the effectiveness of CT.

Symantec remains committed to continually evolve our technology, processes, and offerings to help keep our customers and the Internet safe. We believe that the steps we have taken will ensure that this type of incident never happens again, and we believe that through broad support for CAA and CT, we can help increase both the prevention and the detection capabilities in the CA ecosystem going forward.

Addendum - October 12, 2015

On October 8, 2015, after follow-on questions from industry partners, we reopened our investigation, and identified a set of test certificates that were not included in our original analysis.

While our current investigation is ongoing, so far we have found 164 additional instances where test certificates were inappropriately issued. All of these test certificates have been revoked. These test certificates were spread over 76 domain owners whom we are in the process of contacting.

Separately, we have identified a set of cases where test certificates were issued for domains that, at the time of issuance, were unregistered. Historically, issuance of certificates for unregistered domains was allowed as part of the CA/Browser Forum Baseline Requirements (the Extended Validation Guidelines did not permit such cases) and we used these domains for testing purposes (example: symantectest01.com). Last year, in the April 2014 update to the Baseline Requirements, the language related to unregistered domains was eliminated. We have determined that we failed to update our test certificate policy documentation to reflect these requirements. As a result, we continued to include certificates for unregistered domains in our test process. We have determined that we have issued a total of 3,073 of such test certificates for unregistered domains since the rule updates to the respective requirements documents. It is important to note that because these certificates were for unregistered domains, the risk was even lower than that of any of our other test certificates. Nonetheless, we have ensured that all such test certificates have been revoked. Additionally, we have updated our policies to explicitly prohibit issuance of this type of test certificate.

As mentioned previously, we are committed to accelerating the adoption of Certificate Transparency logging for all certificates that we issue, by adding support for Organization and Domain Validated certificates, and expect most of that work to be complete by the end of 2015. We have also begun our annual audit process and are expanding its scope in the wake of these recent instances, in order to ensure we have independent confirmation that no other issues remain. We anticipate the audit will take three to six months, and once it is complete we will share any key findings.

We have received requests from the Browser community for the certificate details so they can update their black lists accordingly. The certificate details are available here for their reference:

List of Test Certs of Owned Domains

List of Test Certs of Unregistered Domains

We will be updating this document again with any additional information, once our expanded investigation is complete.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud based systems. Our industry leading expertise in protecting data, identities, and interactions gives our customer's confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.