January 26, 2017

Issue Summary

1. We have assigned the following categories to the certificates identified by Andrew Ayer in his January 19, 2017 post for clarity in the rest of this initial investigation disclosure:
    a. Category A: 4 certificates issued on July 14, 2016 that contain example.com CNs and SANs containing test1.com and testexample.com. These were all revoked on date of issue.
    b. Category B: 6 certificates with the word "test" in the CN or SAN domain name, issued on October 21, November 15, and December 15, 2016. These were all revoked on date of issue.
    c. Category C: 21 expired certificates with O=test issued between January 22, 2010 and May 23, 2012. Nineteen of the certificates were revoked within 6 weeks of issuance. One certificate issued on January 22, 2010 expired on January 22, 2011. One certificate issued on May 23, 2012 expired on May 23, 2013.
    d. Category D: 93 certificates with O=test issued between October 21, 2016 and January 18, 2017. These certificates were all revoked within 30 days of issuance, with the last revocation occurring on January 20, 2017, less than twenty-four hours after Symantec learned of the mis-issued certificates.
    e. Category E: 2 certificates issued with O=test and "crosscert" in the domain names issued on October 24, 2016. These were both revoked on date of issue.
    f. Category F: 1 certificate issued to dev119money.com in the domain name, issued on October 28, 2016. This certificate was revoked on November 23, 2016.
2. All 127 certificates were issued by CrossCert, Korea Electronic Certificate Authority. Because CrossCert is a WebTrust audited Registration Authority (RA), Symantec personnel did not participate in the validation process flow for these certificates.

Immediate Response

1. On Thursday evening PST, January 19, 2017, after becoming aware of this issue, Symantec disabled issuance privileges for all CrossCert staff. All issuance privileges remain disabled.
2. Symantec revoked 31 still valid and active Category D certificates on the morning of January 20, 2017 that were issued between December 28, 2016 and January 18, 2017.
3. Symantec has taken over validation and issuance for all pending and new orders submitted through CrossCert. Symantec's authentication team is fully processing these orders independently. Symantec is not relying on any previous authentication work completed by CrossCert.
4. Due to the severity of this matter, Symantec has disabled issuance in all CrossCert provisioned enterprise accounts. Symantec is re-validating all accounts. New issuance from these accounts is blocked until Symantec's re-validation is complete.

Root Cause

1. Symantec contracted with CrossCert as a Registration Authority to delegate the performance of BR Section 3.2 requirements pursuant to Section 1.3.2 of the BRs. CrossCert's issuing staff completed Symantec's required annual training.

2. For the certificates issued between July 2016 and January 2017, Symantec's compliance checks flagged these orders when they were submitted because they contained the word "test", prohibiting CrossCert RAs from issuing these certificates without obtaining an override from CrossCert management.
3. Our audit logs show that CrossCert management overrode the compliance failure flags. CrossCert did not consult with Symantec on the significance of the compliance failure flags or the decisions to override the flags for any of the certificates. Three of the four certificates in Category A solely included "example" and as a result were not flagged. Nonetheless, these three certificates required standard RA processing, and similar to the flagged certificates including "test", CrossCert did not properly complete verification procedures, yet these certificates were issued anyway.
4. CrossCert's issuance behavior that resulted in Category D and F mis-issuance from October 21, 2016 to January 18, 2017 relates to a new documented service offer CrossCert launched for their customers. CrossCert offered certificates to allow customers to test public root ubiquity before purchasing additional certificates with the customer identity in the organization field. CrossCert has explained to Symantec that they used "test" in the "O" field to enable their customers to easily distinguish these test certificates when requesting revocation of the certificate used for testing. CrossCert did not consult with Symantec prior to introducing this new offering. CrossCert management said that the Category C certificates were also issued for customers' internal testing, although not formalized as a documented service offer at that time.
5. CrossCert management has indicated that the Category A, B, and E certificates, 12 total, were issued for CrossCert internal testing.
6. No internal Symantec software testing tool (including the tool subject to management approval and requiring elevated privilege) was involved, as no partners have access to those tools.

Additional Follow-up

1. Symantec has engaged CrossCert daily throughout this investigation. We have requested documentation for our review for all categories, with A, B, and E as highest priority.
2. We have spoken with Ernst & Young Korea, who conducted CrossCert's most recently published unqualified WebTrust audit. We are reviewing E&Y's audit work, including E&Y's detailed approach to ascertaining how CrossCert met the required control objectives. The CrossCert E&Y unqualified audit report for the period ending June 30, 2016, is published at https://cert.webtrust.org/SealFile?seal=2168&file=pdf.
3. We are reviewing all our RA partners, beyond their completed WebTrust audits, including issuance privileges and other controls. We are also highlighting this issue as Symantec communicates with our other audited RA partners that have issuance privileges to reinforce the requirements for proper authentication and issuance, explain the harm caused to the web PKI if those requirements are not followed, and to further emphasize the importance of the safeguards we have in place to prevent these failures.
4. Our investigation of this matter continues, and includes a review of our delegated RA controls and why we did not detect this problematic behavior before it was reported to us. Our findings will feed into our continuous efforts to strengthen controls via automation and process.