Sectigo Certificate Revocation/Reissue

Incident Report for InCommon Certificate Service (August 26-31, 2019)

October 3, 2019

Summary

On August 26, Sectigo was notified of an issue with serial numbers on certain EV certificates. These certificates included serial numbers consisting of all zeros. CA/Browser Forum requirements (see Section 9.2.4), which govern Certificate Authorities like Sectigo, require revocation of these certificates within five calendar days.

While this issue had no security implications, it required the emergency reissuance of 1,095 EV certificates to 85 InCommon participants. As part of this process, Sectigo has corrected all CA/B Forum issues relating to all InCommon EV certificates.

Problem

Sectigo completed a root cause analysis and found a legacy requirement in the Sectigo Certificate Manager (SCM) that a company registration field had to be non-null when entered. Sectigo reports that, for a period of time, this field was populated with all zeros. Because validators were accustomed to seeing “0” entries in other sectors (such as government entities), validators missed correcting data for these for subscribers. When an EV certificate with all zeros in the field was called to the attention of Sectigo, CA/B Forum requirements, as noted above, required revocation within five calendar days. Unfortunately, this occurred just before Labor Day and coincided with the beginning of the new school year at many of the 85 affected institutions.

Resolution

Sectigo re-validated all affected organizations, re-issued all affected certificates, and created a scripted installation solution that required involvement of each impacted institution.

InCommon created a communication plan to assist Sectigo with connecting to the affected organizations:

Tuesday (8/27)

- InCommon sent an email to affected RAOs (Registration Authority Officers) and those in the InCommon Executive role, outlining the problem and the solution.
- Sectigo sent an email to two RAOs from each affected organization with details on the revoked certificates. RAOs were asked to schedule a call with Sectigo to resolve the problem.

Wednesday (8/28)

- Sectigo created a ticket for each institution to facilitate follow-up and began scheduling calls with RAOs.
- Sectigo and InCommon began calling RAOs and others at affected organizations at 3pm ET.
    - Sectigo also started meeting with RAOs that had previously scheduled a call.
    - InCommon called organization executives to alert them of the issue.

Thursday (8/29)

- Contact calls and certificate reissuance continued.

Friday (8/30)

- Sectigo had reissued all affected certificates by Friday (within the CA/B Forum window).

Saturday (8/31)

- Sectigo reissued less than ten certificates for two campuses to address a certificate signing request issue.

Incident Considerations: External and Internal

External Considerations

1. The issue occurred during the beginning of fall semester for many schools.
2. The issue occurred just prior to a holiday weekend (Labor Day), which we anticipated would hamper institution availability
3. There was a very short timeframe (five days) to reissue certificates due to CA/B Forum requirements.
4. An approaching major hurricane was distracting to those in the southeastern U.S.

Internal Considerations

1. Some affected institutions were confused about the process for getting help (e.g. should they schedule a time with Sectigo or wait for affected certs to be re-issued in the Sectigo Certificate Manager).

2. InCommon and Sectigo sent communications to a list of RAOs; the list was later discovered to be incomplete. As a result, some organizations did not receive this communication in a timely manner.
3. Sectigo missed a number of the initial appointments with institutions, however the affected organizations were contacted directly to follow up and complete installation within 24 hours.
4. Additional certificate validation discrepancies were discovered during the reissuing process, requiring Sectigo to re-validate affected certificates.

Impact

Across 85 institutions, there were 1,095 affected EV certificates. This had a significant impact on Sectigo, InCommon, and subscriber daily operations, including unplanned urgent actions and emergency communication within institutions from executives to other staff during an extremely busy time of year. Fortunately there were no security implications or certificate mis-issuance.

InCommon logged 172 staff hours on this incident.

- 935 tickets and emails were received and answered

Sectigo logged 1,308 staff hours on this related incident.

Status and Follow up

Current status is *Resolved*

Sectigo has corrected all CA/B Forum issues relating to all InCommon EV certificates.

Follow-up Actions

Operational improvements

1. Sectigo has automated internal policy checks and uses the external lint checkers, but the internal policy checks were not updated to catch this error of zeros appearing in subject:serialNumbers long ago. That has been done.
2. Sectigo has conducted an audit and found no additional CA/B Forum compliance issues with the existing issued InCommon Certificates.
3. Planned actions
    a. Document critical incident procedures (Jointly)
    b. Complete After Action Report (Jointly)
    c. Held community discussion call on October 11, 2019 with affected community members and InCommon and Sectigo representatives.
    d. Establish a current email notification list of all active RAOs to facilitate future operational communications. (Jointly)