Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Report Status	Final Report
Report Classification	**Public**
Report Date	V1.2 November 27, 2019
Number of Pages	8

Document Versions

Version	Change Date	Modification Comments
1.0	November 18, 2019	First version
1.1	November 21, 2019	After certificate revocations and further analysis
1.2	November 27, 2019	Final version

Table of Contents

1. Incident Report Analysis

1.1 How HARICA first became aware of the problem

During the internal quality checks and tests to introduce improved linting software, it was discovered that three (3) EV TLS certificates were issued without L or ST in the subjectDN.

1.2 A timeline of the actions HARICA took in response

The problematic certificates were all issued from a recently created QWAC certificate profile. The QWAC certificate profile was configured to require at least localityName.

Additionally, it was discovered that the issuing CA was linked to certlint linter instead of the recommended cablint linter. The CA configuration was updated to use cablint linter.

All Issuing CAs technically capable of issuing TLS Certificates were scanned to ensure that the recommended linter was enabled. Only one Issuing CA was affected. All certificates issued from this CA were scanned and re-linted to confirm that no other certificate was issued in error.

Here is a detailed timeline:

Sunday, November 17, 2019

- During internal quality checks due to testing of a new linting software, it was discovered that three (3) EV Certificates using a recently created QWAC profile did not include localityName or stateOrProvince attribute in their subjectDN field.
- Further investigation revealed that the QWAC certificate profile did not enforce "localityName or stateOrProvince" (conditional rule) to be present in the subjectDN of end-entity certificates.
- As a temporary measure, all certificate profiles technically capable of issuing OV/IV/EV/QWAC TLS certificates were updated to enforce the existence of localityName.
- The issuing CA (https://crt.sh/?caid=119883) was linked to certlint linter instead of the recommended cablint linter. However, all previously executed quarterly audits were using the recommended linter (cablint) as it was a separate process. The last internal audit was executed with certificates issued until 2019-09-30 and did not reveal any mis-issuances.
- EV/QWAC Certificate issuance was stopped.
- The CA configuration of the issuing CA (https://crt.sh/?caid=119883) was updated to use cablint for pre-signing linting.
- All Issuing CAs technically capable of issuing TLS Certificates were scanned to ensure the recommended linter was enabled. The scan confirmed that only one Issuing CA was affected (https://crt.sh/?caid=119883). All certificates issued from this CA were scanned and re-linted to confirm that no other certificate was issued in error.
- A notification to Bugzilla was drafted and submitted (https://bugzilla.mozilla.org/show_bug.cgi?id=1597135).

- A notification to affected subscribers was drafted.

Monday, November 18, 2019

- EV/QWAC Certificate issuance was re-enabled.
- Our auditor was notified about the incident, the preliminary findings and planned actions.
- The affected parties were contacted to replace their Certificates within the revocation timeline according to the Baseline Requirements.
- The post-subCA creation ceremony script was updated to include steps that update the crt.sh mis-issuance check script with the new subCA.
- PrimeKey was contacted to request a feature to enable a conditional configuration check, to require subjectDN field (localityName OR stateOrProvinceName) for end-entity profiles.
- The Validation Specialists were particularly noted that for EV Certificates and QWACs the JoI Locality OR StateOrProvince is required, and that these are not related to the subjectDN:localityName, subjectDN:stateOrProvince (the LocalityName and/or StateOrProvince must be copied in both locations).
- The training material for Validation Specialists was scheduled to be updated by end of the week (November 22, 2019) to explicitly describe this requirement to avoid future misunderstandings.
- The certificate with serial number 06607994DD3087EAECDA6184FD21E7B0 was revoked.
- The remaining affected certificates were scheduled to be revoked on Thursday, November 21, 2019.

Tuesday, November 19, 2019

- Further analysis of the incident was conducted. The incident analysis was documented in more detail.
- Additional information related to the incident was posted to the Bugzilla bug.

Thursday, November 21, 2019

- Certificates with serial numbers `41F7531AB378BA72F082AB5B0CB6150C` and `1DEB0CC305A21A74B1527363548084D6` were revoked.

Friday, November 22, 2019

- Training documentation was updated with this particular incident explanation and clear instructions for Validation Specialists. New related questions were added to the test options.

Tuesday, November 27, 2019

- Final report was posted to Bugzilla.

1.3 HAS HARICA STOPPED, OR HAS NOT YET STOPPED, ISSUING CERTIFICATES WITH THE PROBLEM?

Yes. The affected subCA was configured to use the recommended linter in order to technically enforce all applicable EV requirements. Additionally, the certificate profiles were updated to require at least the localityName to appear in the subjectDN field for IV/OV/EV/QWACs and Validation Specialists have been particularly noted for this requirement. Misissued certificates were all revoked by Friday November 22, 2019, within the required time frame.

1.4 A SUMMARY OF THE PROBLEMATIC CERTIFICATES

A full list is included in the next section.

1.5 THE COMPLETE CERTIFICATE DATA FOR THE PROBLEMATIC CERTIFICATES

The entire certificate database was examined. Here are the problematic certificates:

- https://crt.sh/?id=2034062094
- https://crt.sh/?id=1952703527
- https://crt.sh/?id=1991787024

1.6 EXPLANATION ABOUT HOW AND WHY THE MISTAKES WERE MADE OR BUGS INTRODUCED, AND HOW THEY AVOIDED DETECTION UNTIL NOW

The pre-issuance lint for the Issuing CA that issued the problematic certificates was not configured to use the recommended linting tool and the mis-issuance was not immediately detected. Our last quarterly audit scan included Certificates issued between 2019-07-01 and 2019-09-30.

1.7 EXPLANATION ABOUT HOW AND WHY THE MISTAKES WERE MADE OR BUGS INTRODUCED, AND HOW THEY AVOIDED DETECTION UNTIL NOW

There were three causes that were detected in our analysis, all of which occurred for the issue to take place:

1. The Validation Specialist that issued the QWACs mistakenly thought that the jurisdictionOfIncorporationLocalityName and jurisdictionOfIncorporationStateOrProvinceName were sufficient to convey to the Relying Parties that the organization is located in that specific Locality and State. All Validation Specialists were notified about the requirement to include the subjectDN:localityName OR subjectDN:stateOrProvinceName field in IV/OV/EV Certificates. Their training material was updated to include this clarification. In addition to the specific notification/announcement to all Validation Specialists about the proper way to apply the requirements and the training material update for this specific issue, a review of the entire training material for Validation Specialists was considered in search for other areas of misunderstanding. Given that misunderstandings are the hardest to predict when writing or evaluating training material, we also considered changes in our training practices. The conclusion at this time is that, since we never had a similar incident that was addressed to improper training of our staff, we will make efforts to improve training practices and use more real-life examples in the training material and,

whenever recommended, more collaborative knowledge sharing between different team roles based on different scenarios, especially in cases where technical controls are not feasible and thus, human is the main control.

2. A particular subCA was linked to certlint linter instead of the linter which is recommended for the case (cablint). We decided to introduce harder controls to reduce the human-error factor, thus we updated our linting script to automatically detect whether the lint is for a TLS Certificate subject to the Baseline Requirements and EV Guidelines. This will ensure the recommended linter is automatically selected. The improvement to auto-detect the type of certificate is considered effective to prevent this human error from repeating. We are continuously examining improvements to automate CA configuration in post-ceremony activities based on the types of Certificates that the Issuing CA is technically capable of issuing. HARICA is currently using several available CLI configuration options to automate the post-ceremony CA configuration but EJBCA has certain limitations that cannot be easily performed using CLI.
3. There were technical restrictions posed by the EJBCA software. For other certificate profile requirements (whether fields are required/optional, acceptable values and size per subject attribute, etc), EJBCA provides the necessary tools and HARICA is using them to enforce the Certificate Profiles per the Baseline Requirements and EV Guidelines. The only rule that EJBCA was not able to provide in the end-entity profile tools was the combination of existence of subject:LocalityName OR subject:StateOrProvinceName. To address this lack of support in the EEP configuration, we requested a feature from PrimeKey (https://jira.primekey.se/browse/ECA-8704) to allow for these conditional restrictions in end-entity profiles, as this is a feature that most publicly-trusted CAs would like to use. Until then, we set our end-entity profiles for issuance of TLS Certificates to require subject:localityName for IV/OV/EV/QWACs (in addition to the other required fields).

2. Incident Impact

This incident had impact on two Subscribers where certificates had to be replaced. No other impact was detected.

3. Conclusions and Recommendations

We consider the mitigations applied to be sufficient to prevent similar issues from taking place in the future, but we will closely monitor to verify. HARICA is continuously improving its technical controls to restrict certificate profiles according to the Baseline Requirements and EV Guidelines. The limitation of EJBCA to restrict certificate to include “localityName OR stateOrProvince” is now a feature request to the software vendor, PrimeKey. In the meantime, HARICA configured the end-entity profiles related to IV/OV/EV/QWACs for TLS Certificate to require subject:localityName.

We re-affirmed our strategy to use more automation and remove the possibility for human errors in as many places as possible. Despite the failure of 2 controls (training, pre-linting) and EJBCA’s limitation to enforce this specific rule, this issue was caught by HARICA because of multiple

layers of control (internal checks/testing). This testing was conducted as part of our continuous preemptive actions to introduce improved tools (linters in this case) and more automation. With respect to the quality and completeness of the training practices, we consider that training people with more real-life examples is the key to avoid mis-understandings or improper handling of corner cases. We are continuously trying to learn from existing incidents and improve our existing tools and practices.

4. About this document

This document is considered **public**.

This document has been approved by **HARICA's Policy Management**.