Hellenic Academic and Research Institutions

Public Key Infrastructure

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Report Status	Interim Report
Report Classification	**Public**
Report Date	V1.0 November 18, 2019
Number of Pages	6

Document Versions

Version	Change Date	Modification Comments
1.0	November 18, 2019	First 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 Immediate actions

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

In addition to this, 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.

1.2.1 Timeline of the actions HARICA took in response

Sunday, November 17, 2019

- During internal quality checks due to testing 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 affected certificates are scheduled to be revoked on Thursday, November 21, 2019.

1.3 Is the problem solved?

Yes. The affected subCA has been configured to use the recommended linter in order to technically enforce all applicable EV requirements. Additionally, the certificate profiles have been 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. Mis-issued certificates shall be revoked until Thursday November 21, 2019 (within the required time frame).

1.4 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

1.5 Why were these problems not detected sooner?

The pre-issuance lint for the Issuing CA that issued the problematic certificates was not configured to use the recommended linting tool.

1.6 ACTIONS TO PREVENT RECURRENCE OF THIS ISSUE

There were two problems that were detected in our root cause analysis:

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.
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. In addition, we configured the end-entity profiles capable of issuing IV/OV/EV/QWACs to require the subjectDN:localityName to appear in the Certificate until a better technical control is offered by the software vendor. We submitted a feature request to PrimeKey το enable the combined check for localityName OR stateOrProvinceName.

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 already has technical controls in place 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.

4. About this document

This document is considered **public**.

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