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	V1.1 March 7, 2019
Number of Pages	6

Document Versions

Version	Change Date	Modification Comments
1.0	Feb 27, 2019	First Version
1.1	Mar 7, 2019	Final report after revocation of affected CA Certificates

Table of Contents

1. Executive Summary

On February 25th 2019 during a detailed policy documents review comparing differences between the Baseline Requirements and Mozilla Policy, we discovered that HARICA had issued Intermediate CA Certificates with ECDSA P-384 key and SHA256 hashing algorithm which is a violation of Section 5.1 of the Mozilla Root store Policy.

The effective date of the Mozilla Root store Policy that only allows specific curve-hash pairs was February 28, 2017. Please note that this issue is not considered a violation of the Baseline Requirements which describe allowed curves and hashing algorithms in section 6.1.5.

HARICA's CA Software (EJBCA) was set to inherit the Root CA's combination of Key and hash algorithms and used the SHA256ECDSA algorithm although the key was using curve P-384. This led to issuing subCA Certificates and end-entity certificates with the same pair (SHA256, P-384).

As soon as the finding was verified and an internal Incident created (Ticket#20190226100002302), Certificate issuance was disabled from the affected subCAs.

A full database scan was conducted and revealed only one (1) affected end-entity certificate issued for a test web site operated by HARICA. Five (5) intermediate CA Certificates were also affected.

Mitigation measures have already been implemented to minimize the risk of reoccurrence. More details in section 2.7 of this report.

The problematic Certificates were revoked at March 6th, 2019.

2. Incident Report Analysis

2.1 How HARICA first became aware of the problem

On February 25th 2019 during a detailed policy documents review comparing differences between the Baseline Requirements and Mozilla Policy, we discovered that HARICA had issued Intermediate CA Certificates with ECDSA P-384 key and SHA256 hashing algorithm which seemed to be in contradiction with the 3rd bullet of Section 5.1 of the current Mozilla Root store Policy).

2.2 Immediate actions

The Security Manager was notified about the finding who immediately investigated this issue and determined that the finding was accurate and in violation of the current Mozilla Root store Policy. The operations team was notified to block the capability of end-entity certificate issuance from the CA software.

2.2.1 Timeline of the actions HARICA took in response

Monday, February 25, 2019

- Finding was detected and reported to Security Manager along with supporting evidence (policy documents, changes on github, effective dates)
- Security Manager confirmed the finding and declared it an incident

- Operations were informed to block issuance from affected subCAs

Tuesday, February 26, 2019

- Mozilla Module owner was notified
- Certificate database analysis was performed to detect affected Intermediate and end-entity certificates. Only one certificate issued for HARICA test URL was affected (and unexpired and unrevoked) so there was no need to notify Subscribers.
- Revocation of affected CA and end-entity certificates was scheduled for week 4-8 March 2019.
- Root cause analysis was performed which revealed that the policy change review process needed improvements.

Wednesday, February 27, 2019

- CA Software was configured to enforce proper hashing algorithms with ECDSA keys flowing down from the ECC Root.
- Bug opened in Bugzilla with Component "CA Certificate Compliance"

Tuesday, March 7, 2019

- A Ceremony took place that included revocation of the affected CA Certificates.

2.3 Is the problem solved?

HARICA has blocked issuance from the affected subCAs. The problem has been successfully mitigated by enforcing the proper algorithms in the CA software.

2.4 Summary of Problematic HARICA Certificates

There are currently one (1) end-entity certificate and five (5) intermediate CA Certificates that are unexpired and unrevoked in scope of the Mozilla Policy that were affected by this incident.

2.5 The complete certificate data for the problematic certificates

The entire certificate database was examined. Here is the complete list of unexpired and unrevoked Certificates in scope of the Mozilla Policy affected by this incident.

End-entity Certificates:

- https://crt.sh/?id=336609534

Intermediate CA Certificates:

- https://crt.sh/?id=12729858) (Issued July 28, 2015)
- https://crt.sh/?id=484579153 (Issued May 23, 2018)
- https://crt.sh/?id=559632568 (Issued June 27, 2018)
- https://crt.sh/?id=1222759697 (Issued Feb 20, 2019)
- https://crt.sh/?id=1222760018 (Issued Feb 20, 2019)

2.6 WHY WERE THESE PROBLEMS NOT DETECTED SOONER?

HARICA uses post-issuance linting for all CA Certificates (using certlint, zlint) but that did not detect the problem. Publishing CA Certificates to CCADB (which finds its way to crt.sh) also didn't raise any alarms. HARICA also uses pre-issuance linting for all end-entity Certificates that also did not detect this divergence.

During policy changes, the policy team carefully reviews the changes introduced by various requirements documents (CA/B Forum documents ETSI requirements, Root store custom policies). In this particular case, the 2nd bullet of section 5.1 of the Mozilla root store policy seemed to allow for SHA-256 and the policy review team incorrectly regarded this section as a re-wording and re-formatting of the previous policy (version 2.3).

2.7 ACTIONS TO PREVENT RECURRENCE OF THIS ISSUE

We modified our internal policy review process so that the policy review team is split in two. Each sub-team will review the changes independently of the other so will have a second independent review cycle when policy changes are introduced from Root store programs in order to better assess policy changes of technical specifications that may impact operations.

We will also ask from our CA software manufacturer to implement specific additional validators for Mozilla Policy requirements that detect similar inconsistencies.

3. Incident Impact

Only HARICA internal Certificates were issued from the affected subCAs, one currently unexpired. We plan on revoking this end-entity and intermediate CA Certificates by March 8th 2019.

4. Conclusions and Recommendations

This incident had no significant impact on HARICA's operations, Subscribers or Relying Parties. However, several opportunities for improvement have been identified and can be summarized in the following recommendations:

- Improve policy review when changes are introduced.
- Improve linting tools to detect additional technical requirements mandated by custom policies such as Mozilla Root store policy.

5. About this document

This document is considered **public**.

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