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	V1.0 Mar 15, 2019
Number of Pages	5

Document Versions

Version	Change Date	Modification Comments
1.0	Mar 15, 2019	Final Version

Table of Contents

1. Incident Report Analysis

1.1 How HARICA first became aware of the problem

During a subCA creation ceremony on 2019-03-06, two Technically Constrained CA certificates (per section 7.3.1 of the Mozilla Policy) were issued that contained a name constraints extension that included non UTF-8 characters. The problematic CA certificates were detected at the post-creation quality verification procedure.

1.2 Immediate actions

After detection of the problem, an investigation was initiated to find the root cause of the problem as there were no indications of misconfiguration.

The CA Certificates were never enabled in the CA platform and were revoked on the next day.

1.2.1 Timeline of the actions HARICA took in response

2019-03-06

- Two subCAs were issued with improper characters in the name constraints extension
- An investigation was initiated that revealed the cause of the problem. To explain further, HARICA decided to add dirName entries in the permittedSubtree attribute with Greek characters (in UTF-8) that should be encoded as UTF8String.
    - The ceremony was performed in a Linux console with locale set to "`en_US.UTF-8`" by default
    - Before executing the issue commands to generate the subCAs, in order to be able to view Greek characters, the CA Administrator during the ceremony proposed to set the environment variable "`LANG=el_GR.UTF-8`" expecting the Greek characters in the name constraints to be readable in the verification process. The proposal was approved and executed.
    - Further discussion took place at that point and it was agreed to revert back to the default value of the LANG variable so that we do not deviate from the approved ceremony script. The CA Administrator should execute "`LANG=en_US.UTF-8`" but instead made a typo and executed "`LANG=el_US.UTF-8`", which is non-existent locale setting. This typo was not detected by the internal auditor or the other members that participated in the ceremony. Also, this typo did not result in any warnings at the console. We discovered it later after reviewing the history of the executed commands.
- The problematic CA Certificates were uploaded to CCADB.

2019-03-07

- A new ceremony was planned and the two subCAs were revoked
- A public incident report was initiated

2019-03-15

- This incident report was approved by management and published to Bugzilla.

1.3 Is the problem solved?

HARICA was able to reproduce the problem in the test environment, identified the cause of the problem and issued the CA certificates correctly.

1.4 Summary of Problematic HARICA Certificates

Two CA certificates were affected.

1.5 The complete certificate data for the problematic certificates

Intermediate CA certificates:

- https://crt.sh/?id=1265291634
- https://crt.sh/?id=1265291467

1.6 Why were these problems not detected sooner?

HARICA always performs the exact ceremony steps in a testing environment before executing the script to production. The tests were completed successfully in the test environment and the produced test CA certificates did not have problematic values in name constraints extension.

1.7 Actions to prevent recurrence of this issue

Ceremony instructions were updated to include a notice that the team must not deviate from the standard script unless absolutely necessary. An additional step added to verify the console locale settings.

2. Incident Impact

This incident had no impact to HARICA's operations, Subscribers or Relying parties.

3. Conclusions and Recommendations

Recommendations for stricter execution of the ceremony script were added in the ceremony instructions. A verification step was added to the ceremony script.

4. About this document

This document is considered **public**.

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