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 Mar 19, 2019

Document Versions

Version	Change Date	Modification Comments
1.0	Mar 14, 2019	First Version
1.1	Mar 15, 2019	Corrections to the executive summary
1.2	Mar 19, 2019	Final report after revocations

Table of Contents

1. Executive Summary

CA/B Forum Baseline Requirements section 7.1 and Mozilla Policy section 5.2 requires serial numbers to include at least 64 bits of entropy from a CSPRNG.

"CAs MUST maintain current best practices to prevent algorithm attacks against certificates. As such, all new certificates MUST have a serial number greater than zero, containing at least 64 bits of output from a CSPRNG".

HARICA uses EJBCA CA software since May 9th 2018. EJBCA uses a default configuration that sets the size of the serial number to 8 bytes resulting in serial numbers with 64 bits. The public discussion in Mozilla-dev-security-policy mailing list (m.d.s.p.) revealed that because the serial number must be a positive number, which means the first bit must be zero, EJBCA effectively uses 63 truly random bits and not 64.

HARICA monitored the discussion in m.d.s.p. and detected that the configuration on EJBCA was using the default values for serial number size, even though this was identified as a compliance issue before migrating to EJBCA in March 2018. The investigation revealed that HARICA had evaluated the results of ballot 164 (that added the current language of section 7.1) and modified in May 2017 the custom -at-the-time- CA software to include 127 bits in the serial numbers of end-entity Certificates, exceeding the requirement of 64 bits. When HARICA migrated to EJBCA on May 9th 2018, it verified that the issued certificates used 64 bit serial numbers that seemed compliant with the requirements of BRs section 7.1. HARICA did not analyze the actual CA software code to evaluate the algorithm that the software vendor used to produce the serial numbers in order to reveal the fact that the first bit of replaced by a zero, thus effectively using 63 bits of entropy. This resulted in issuing certificates with a non-compliant serial number **between 2018-05-04 and 2019-03-05**.

A full certificate database scan was conducted and revealed that 461 SSL/TLS, 4157 S/MIME and 15 CA Certificates (unexpired and unrevoked) had improper serial numbers. In addition to these, 2 SSL/TLS and 62 S/MIME Certificates that had compliant serial numbers but were issued from a CA with improper serial number, are affected by this incident.

Mitigation measures to minimize the risk of reoccurrence have been identified and a timeline of the implementation is under discussion. More details in section 2.7 of this report.

The problematic SSL/TLS Certificates were revoked on March 16th, 2019 according to the revocation timeline of SSL/TLS Certificates mandated in the Baseline Requirements.

The problematic CA Certificates capable of issuing SSL/TLS Certificates were revoked on March 18th, 2019 (along with the compliant end-entity certificates that were issued by these CAs), according to the revocation timeline of SSL/TLS Certificates mandated in the Baseline Requirements.

2. Incident Report Analysis

2.1 How HARICA first became aware of the problem

A discussion in m.d.s.p. related to another subject about a CA's inclusion request, raised some concerns about the Certificate serial numbers produced by CA Software EJCBA. This software is currently used by HARICA. HARICA used to have a custom CA software that fully met the

requirements for the creation of a certificate serial number according to the Baseline Requirements and Mozilla Policy, so certificates created before migrating to EJBCA are not impacted. The e-mail thread in m.d.s.p. broke off in many parallel threads making it difficult to track. The issue was somewhat controversial and the Mozilla community expressed conflicting interpretations. Finally, a clarification was provided on March 10, 2019 by Mozilla CA Certificate Policy Module Owner that this incident should be treated as a violation of Baseline Requirements section 7.1. The discussion is still ongoing and there are some indications that the default configuration of EJBCA is compliant according to a pedantic/ reading of section 7.1. Nevertheless, HARICA considers this a mis-issuance and a compliance issue and treats it as such.

2.2 IMMEDIATE ACTIONS

The discussion in m.d.s.p. made HARICA review the serial number configuration and although this was properly configured in HARICA's custom CA software, when migrated to EJBCA, the default settings were used for the serialNumber size. A configuration file was added on 2019-02-27, therefore all certificates issued after that date, are compliant with section 7.1 of the Baseline Requirements.

2.2.1 Timeline of the actions HARICA took in response

July, 2016

- CA/B Forum voted ballot 164 which became effective 2016-09-30.

May 17, 2017

- HARICA updated the custom CA Software code to produce serial numbers with 127 > 64 random bits from a CSPRNG.

December 1, 2017

- Published a concern/effort to have a way to check for this issue via certlint/cablint as demonstrated in https://github.com/awslabs/certlint/issues/56

May 9, 2018

- HARICA migrated to EJBCA.

February, 2019

- Monitored discussions in m.d.s.p. related to DarkMatter and the discussion about serial number size/entropy.

February 27, 2019

- Detected that HARICA's production EJBCA was missing the necessary configuration file "`cesecore.properties`" to ensure that new serial numbers have more than 64 bits of entropy from a CSPRNG.
- The missing configuration file was immediately added, and Certificates issued after that date include 16-byte serial numbers that effectively have at least 120 bits of entropy from a CSPRNG.
- At that time, HARICA didn't treat this as a non-compliance but as a concern pending further clarifications. HARICA continued to monitor the m.d.s.p. discussions and contacted other experts to seek their opinion, especially on the security context of the

discussed topic and possible threats for produced certificates that might affect Relying Parties.

Saturday, March 9, 2019

- HARICA requested clarifications from Mozilla CA Certificate Policy Module Owner via m.d.s.p. about whether the finding of getting 64 bits of entropy and replacing the first bit with zero violates section 7.1 of the Baseline Requirements.

Sunday, March 10, 2019

- Mozilla confirmed they consider that EJBCA effectively uses less than 64 bits of entropy in the serial number creation in violation of section 7.1. of the Baseline Requirements.
- An official investigation was launched to determine the impact of existing certificates to Relying Parties.
- The investigation revealed the facts listed in this timeline.
- The investigation included a security analysis. The analysis concluded that that there was no practical security concern (collision attack) for Certificates issued with the problematic serial numbers because only the SHA-2 family of hashing algorithms were used for signatures and the collision resistance is considered sufficient. Regardless of our internal security analysis, the fact that BRs section 7.1 was updated by ballot 164 to mitigate against MD5 and SHA1 collision attacks, was reassuring. Based on the discussions in m.d.s.p. about this topic, the common understanding of the community is similar; that this was more of a compliance issue.

Tuesday, March 12, 2019

- A search for non-compliant SSL/TLS unexpired, unrevoked Certificates was conducted. The search revealed that **461 SSL/TLS** Certificates were affected.
- A second search for non-compliant S/MIME unexpired, unrevoked Certificates was conducted. The search revealed that **4157 S/MIME** Certificates were affected.
- A third search for non-compliant unexpired, unrevoked CA Certificates in scope with BRs and Mozilla Policy was conducted. The search revealed that **15 CA Certificates** were affected.
- A forth search for all unexpired, unrevoked Certificates issued from CA Certificates capable of issuing SSL/TLS Certificates. The search revealed that **2 SSL/TLS** and **62 S/MIME** Certificates that were fully compliant with the BRs (including compliant serial numbers) were affected.
- An incident report was initiated for public use.

Wednesday, March 13, 2019

- The SSL/TLS Subscribers were notified that they would need to replace their certificates as soon as possible and that their currently valid certificates with problematic serial numbers shall be revoked automatically on Saturday March 16, 2019.
- The Conformity Assessment Body was notified about the escalation of the issue and preliminary findings were disclosed.

Thursday, March 14, 2019

- Replacement Intermediate CAs were issued
- This incident report was approved by management and published to Bugzilla.

Saturday, March 16, 2019

- **461 SSL/TLS** with problematic serial numbers were revoked between 08:46 and 08:52 UTC

Monday, March 18, 2019

- **2 SSL/TLS** Certificates with compliant serial numbers were revoked because they were issued from a CA that was technically capable of issuing SSL/TLS Certificates
- **62 S/MIME** Certificates with compliant serial numbers were revoked because they were issued from a CA that was technically capable of issuing SSL/TLS Certificates
- **6 Intermediate CA** Certificates technically capable of issuing SSL/TLS Certificates were revoked
- These Certificates were revoked between 12:31 and 12:34 UTC.

2.3 IS THE PROBLEM SOLVED?

HARICA issues compliant serial numbers in Certificates since 2019-02-27.

2.4 SUMMARY OF PROBLEMATIC HARICA CERTIFICATES

There are currently 461 end-entity certificates for SSL/TLS, 4157 end-entity certificates for S/MIME and 15 intermediate CA Certificates that are unexpired and unrevoked 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 affected by this incident.

End-entity SSL/TLS Certificates:

- See attachment "valid-TLS-certs-with-insufficient-serial-entropy@2019-03-12.csv" that includes serial numbers and SHA1 fingerprints of Certificates. SSL/TLS certificates are already published in at least two qualified CT logs meeting Google and Apple CT Policy.

End-entity S/MIME Certificates:

- See attachment "valid-SMIME-certs-with-insufficient-serial-entropy@2019-03-12.csv" that includes serial numbers and SHA1 fingerprints of Certificates.

Intermediate CA Certificates:

1. https://crt.sh/?id=909718586
2. https://crt.sh/?id=136162953
3. https://crt.sh/?id=1222760197
4. https://crt.sh/?id=136162952
5. https://crt.sh/?id=559632566
6. https://crt.sh/?id=136162955

7. https://crt.sh/?id=1222759700
8. https://crt.sh/?id=484579146
9. https://crt.sh/?id=1222761078
10. https://crt.sh/?id=1222759726
11. https://crt.sh/?id=1222759690
12. https://crt.sh/?id=559632567
13. https://crt.sh/?id=1222759679
14. https://crt.sh/?id=1222760114
15. https://repo.harica.gr/certs/HaricaEcclesiasticalAcademyofVellaClientSubCAR1.pem with SN 6a042ec821d7be27 and SHA1 F10A849BA720DFD528EFFB91399CECE0557D8D7E

Compliant end-entity Certificates that were issued from an Intermediate CA Certificate with incorrect serial number and technically capable for issuing SSL/TLS Certificates:

- See attachment "impacted-TLS-certs-from-CA-revocation@2019-03-15.csv" that includes serial numbers and SHA1 fingerprints of Certificates.
- See attachment "impacted-SMIME-certs-from-CA-revocation@2019-03-15.csv" that includes serial numbers and SHA1 fingerprints of Certificates.

2.6 WHY WERE THESE PROBLEMS NOT DETECTED SOONER?

HARICA followed the instructions of the CA software vendor and reviewed that the default configuration produced 64-bit random serial numbers. A detailed code analysis for the functions that create the serial number would have revealed the fact that effectively less than 64 bits of entropy were included in the serial number.

The serial numbers appeared compliant and met RFC 5280. Also, the checks of commonly-used linting tools (cert/cablint, zlint) did not detect or warn about a serial number failure. HARICA reported an issue https://github.com/awslabs/certlint/issues/56 for cert/cablint on Dec 2017 related to the serial number, and the fact that small serial numbers were not being effectively detected. The author had provided a technical explanation about the difficulties of creating such a check.

2.7 ACTIONS TO PREVENT RECURRENCE OF THIS ISSUE

HARICA already has a policy to exceed the minimum technical requirements and practices when feasible and will exercise stricter evaluation of configuration parameters in components produced by third-party vendors (even those shared among most CAs, thus more broadly tested and evaluated).

3. Incident Impact

A large number of HARICA Subscriber Certificates were affected. All SSL/TLS affected Subscribers were notified that their problematic certificates must be replaced by Saturday March 16th 2019. The affected SSL/TLS certificates are scheduled to be revoked automatically on that same date. Some S/MIME affected Subscribers were notified that their problematic certificates must be replaced by Monday March 18th 2019. The affected 62 S/MIME certificates are scheduled to be revoked automatically on that same date.

4. Conclusions and Recommendations

This incident had a significant impact on HARICA's operations, Subscribers and possibly Relying Parties due to the strict revocation timeline requirements mandated by the Baseline Requirements, even though the security threat to Subscribers and Relying Parties was negligible. However, the rules of the Baseline Requirements (section 4.9.1.1 listed item 7 and 4.9.1.2 listed item 5) leaves no room for not revoking Certificates in the BR's scope when there is a violation of these Requirements. Some Subscribers are expected to fail to install the replacement certificates before the end of the 5-day requirement, leading to availability problems of their offered services. Opportunities for improvement have been identified and can be summarized in the following recommendations:

- Engage in CA/B Forum to discuss about the revocation requirements (the 5-day revocation requirement for end-entity certificates and 7 days for CA Certificates) for situations where there is negligible security risk associated with an incident, that would allow CAs to file incident reports and have different revocation timelines (or no revocation at all) per incident severity, accompanied with good examples to guide the assessment or have documented criteria to make assessment as objective as it can be.
- Improve Subscriber awareness and especially the fact that they need to be in a position to replace their certificates when the CA notifies there is either a security risk or a compatibility issue.
- Subscribers should use automated tools to manage their certificates, especially in large deployments.
- Improve linting tools to detect additional technical requirements mandated by policies such as the Baseline Requirements and the Mozilla Root store policy.

5. About this document

This document is considered **public**.

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