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 September 12, 2018
Number of Pages	8

Document Versions

Version	Change Date	Modification Comments
1.0	Sep 12, 2019	First Version

Table of Contents

1. Executive Summary

The CA/B Forum Baseline Requirements section 4.9.10 states that:

"If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder SHOULD NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

Effective 1 August 2013, OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 MUST NOT respond with a "good" status for such certificates."

In the case of pre-certificates as described in RFC 6962, there is an expectation that if a pre-certificate has been issued, a final certificate must be issued as well. However, there are legitimate cases where the CA may decide to abort the issuance of a final certificate if, for example, a pre-certificate cannot be submitted to a certain number of CT logs in order to obtain the necessary number of SCTs to be embedded in the final certificate. This lead the OCSP service to respond to queries for these particular pre-certificates with the status "unknown". This is considered to be confusing to Relying Parties because the CA should be knowledgeable whether the final certificate was issued (thus should return status "valid") or not (in which case the certificate should return status "revoked").

HARICA monitored the discussion in m.d.s.p.

- https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/FB-SfaY040c

and detected that the CA software (EJBCA) treats pre-certificates that did not lead to the creation of final certificates as "unknown", and this is the state the OCSP Responders use when a Relying Party checks the status of such a certificate.

There were arguments supporting that this was in fact a violation and arguments that it was not. Even though this incident has no impact on Relying Parties or Subscribers, on September 10 2019 HARICA decided to treat this as a compliance issue and contacted PrimeKey in order to provide guidance so that OCSP responders return the status of "revoked" for pre-certificates for which there is no corresponding final certificate.

A full certificate database scan was conducted and revealed that **96** pre-certificates were affected.

We created a script to update the certificate database in order to mark the affected pre-certificates as "revoked".

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

2. Incident Report Analysis

2.1 How HARICA first became aware of the problem

Let's Encrypt filed an incident report and a discussion took place in m.d.s.p. about the status of pre-certificates returned by OCSP responders.

2.2 Immediate actions

Since this incident had no immediate impact on Relying Parties or Subscribers, we studied the various RFCs and requirements and concluded that the expectations of Relying Parties when

checking the status of a pre-certificate is to get either “valid” or “revoked”. It doesn’t make sense for a CA to respond with “unknown” because, based on RFC 6962, the CA “promises” to issue.

2.2.1 Timeline of the actions HARICA took in response

Wednesday, September 10, 2019

- After monitoring the discussion in m.d.s.p. and evaluating the various RFCs and requirements, the Security Manager declared it an incident.
- Bug 1580393 was opened in Bugzilla with Component “CA Certificate Compliance”.
- PrimeKey was informed via ticket to provide guidance for detecting the problematic cases of pre-certificates leading to status “unknown” and how to update the information.
- PrimeKey provided a public link with steps to detect and update the database.

Thursday, September 11, 2019

- Operations used the information from PrimeKey in order to automate the process by creating scripts, and tested the accuracy and effectiveness of those in the staging environment.
- An analysis was performed in the production Certificate database to detect affected pre-certificates. 96 cases were detected.

Friday, September 12, 2019

- Operations confirmed that the OCSP responders returned “unknown” for all affected pre-certificates.
- The database was updated to set the status to “revoked” for the affected pre-certificates.
- Operations confirmed that the OCSP responders returned “revoked” for all affected pre-certificates.

2.3 IS THE PROBLEM SOLVED?

The problem is currently mitigated by executing the detection script on a daily basis. This is expected to be fully fixed in an upcoming release of EJBCA. However, we consider this mitigation effective and efficient for this particular issue.

2.4 LIST OF PROBLEMATIC HARICA PRE-CERTIFICATES

Here is a list of the serial numbers of affected pre-certificates:

1. 1F3B487F0327ABFA
2. 244B051A2301F79F
3. 2532DDF452545761
4. 25C752C86885E9CD
5. 26D1CB870B22072A

6. 3E2454A20AD91B57
7. 5544766AE10C67D3
8. 610CFAFCD17C7B3D
9. 6A1121210417226A
10. 7447CE05969AFC77
11. 76E6A4946950888
12. 7D946D11B7EAF252
13. B8D382D2186962B
14. 1EBFBB17DEDC9E91
15. 23AD37D7D58C054D
16. 43A415554DA53F2D
17. 4A94359314426D44
18. 4DA22829FA9FA5C
19. 587EB685D146C059
20. 59B40216EBE00233
21. 66338CB45AD2BFBB
22. 7D494EFC8529FCBE
23. B3C2B3DA6C635A1
24. 15463A46170550 8E
25. 16465BBB1C77E847
26. 1B271A17DE8A40AC
27. 20029A7D008BFCEF
28. 2DFCA8124132DDE4
29. 306CECD27DC55CD1
30. 33FBD24668D48E72
31. 40D356547CAD8578
32. 45439CEB13DB787A
33. 45F61562EBB2616
34. 4DFC5690252B00E5
35. 5336D381418ABDC1
36. 56AC8208AD5BA5B3
37. 60B97370FE15E12D
38. 63EB0A99B7CFF88C
39. 6434FAC8DD603A4A
40. 70C0400500A7ABE6
41. 7678B9AE1987D454
42. ECAE5DAF321F80F
43. FA7B4640192B003
44. 2394E0D943FD4A00
45. 4C8F2B0B7990C355
46. 6828783E9D7BE7D4
47. 76E1697EE356DFEB
48. 20A139DE39985C78
49. 16063094F8C57E99
50. 1EA0DD18CC69F593
51. 21BC3C81C9BBF7B9
52. 23E0AB2B9F760A14
53. 274B07A0FF2CD870
54. 293024099812B13
55. 29AAF5E322CD7C9A
56. 2B4878BB258EA4AD
57. 3A4B76CD2137AF88

58. 3A71C589F8D0A3FC
59. 3BA255BD56E92657
60. 40BA14B037DC635C
61. 4391F18245447B54
62. 44E7271160A85CC0
63. 457149FA5B89D383
64. 4B60C0ACDA8CF53E
65. 5D5FCEBBB60D827E
66. 61AF0B1A1FA61691
67. 63E2966E777AE7AE
68. 640816CFD48AEB91
69. 6C9E63FEB0DCC2DE
70. 6CE09D086313AF4A
71. 6F1B70140BCE68D0
72. 70D66E24C3AC014
73. 7628601B7B7C302B
74. 78312155EBE48937
75. 7859D14E0331CA06
76. 913ACC9F79C6677
77. A1F0410589CBFB
78. C8428260EAD7333
79. 10ACA895F8C9C3F4
80. 174BA55C7F061841
81. 1794BC1842CE0134
82. 1D31DE041F3E9374
83. 2B696D88F46E87AF
84. 39E05BDEB605D810
85. 406DE077146E9602
86. 48B902396A6E21A2
87. 48F964CF99837688
88. 623A2F1B1092EEB2
89. 6337FF00AF9DA2F9
90. 6D88F2BD2A0420DB
91. 6DF8C4FD6CDD22E2
92. 7706780B11C45604
93. 7DD6479E4105BBAE
94. 93725666F11CCA6
95. D1FFA7A836CDFB
96. ECB04E97DFD7361

2.5 THE COMPLETE CERTIFICATE DATA FOR THE PROBLEMATIC PRE-CERTIFICATES

The entire certificate database was examined. Here is a sample of some of these pre-certificates.

- https://crt.sh/?id=478180310&opt=ocsp
- https://crt.sh/?id=463609678&opt=ocsp
- https://crt.sh/?id=451364638&opt=ocsp

2.6 WHY WERE THESE PROBLEMS NOT DETECTED SOONER?

HARICA did not consider this a requirements violation because the final certificate was not issued, therefore the status "unknown" was appropriate per RFC 6960. A different interpretation was provided by the community by combining this with RFC 6962 which made us re-evaluate the issue.

2.7 ACTIONS TO PREVENT RECURRENCE OF THIS ISSUE

We created a script that detects whether a pre-certificate is issued and not the corresponding final certificate.

3. Incident Impact

Pre-certificates cannot effectively be used by Subscribers and by definition they are not trusted by Relying Parties. There was also no impact to operations; certificate issuance continued without interruptions.

4. Conclusions and Recommendations

This incident had no impact on HARICA's operations, Subscribers or Relying Parties. We have no further recommendations to the community other than to emphasize the difficulty in interpreting combined requirements from multiple sources (RFCs, CA/B Forum requirements, Root Program Policies, Auditable Standards).

HARICA decided to publicly disclose the script that identifies the pre-certificates which did not lead to a final certificate. This script will be sent to PrimeKey for validation and if it is considered safe and accurate by PrimeKey, CAs using EJBCA may obtain it and use it at their own risk.

5. About this document

This document is considered **public**.

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