CAB Forum Bratislava, February 2020

Browser News - Mozilla

A Program Manager

Wayne Thayer has left Mozilla. Mozilla is planning to hire a replacement, and Kathleen expects to have the new job requisition posted soon. Meanwhile, Wayne is continuing to represent Mozilla at the CA/Browser Forum and as the Module Owner for the CA Certificate Policy in a volunteer capacity. Please contact Kathleen with any questions.

B Inclusion Request Status

Kathleen is approximately 2 months behind on reviewing CA updates to root inclusion requests. If you have submitted updated information within the past 2 months, please be patient. Kathleen expects this to get worse while the CA Program is understaffed. Expect extra delays in the root inclusion process until a replacement for Wayne is hired.

C Root Store Policy

Version 2.7 of Mozilla's Root Store Policy went into effect on January 1st, and a summary of the changes may be found in Mozilla's security blog posted December 11. Thank you to all who contributed to the discussions. If you have suggestions for future improvements, please create an issue on the GitHub repository.

D CA Communication Survey Results

Mozilla sent a communication and survey to all CAs in our program in early January. The responses have been published on a wiki page.

Thank you to everyone who completed the survey. All 53 CAs in Mozilla's program have responded, and all but 2 responded without additional follow-up.

All CAs have committed to bring their CP/CPS into compliance with the new Mozilla policies by 1-April. This is quite an improvement over past policy updates after which some CAs chose to wait for their next annual review before coming into compliance.

All CAs also agreed to comply with the new requirement for EKUs in end-entity certificates issued after June 2020.

The most comments were received on action #5 regarding Intermediate Audit Letter Validation (ALV) results. Kathleen has published guidance for resolving these issues in the Acceptable Remediations section of the ALV wiki page. **If ALV has correctly detected that your audit statement(s) are missing the SHA-256 thumbprint of an intermediate certificate, then you must file an incident report.** Obtaining a revised audit statement,

revoking the certificate, or adding it to OneCRL are listed as the acceptable forms of remediation for this issue - see the wiki page for details.

E Updated Incident Reporting Guidance

Based on feedback from Jeff Ward during the Guangzhou meeting, additional guidance on incident reporting has been added to the wiki. It now states that CAs should submit a separate incident report when:

- Mozilla policy requires that the CA revoke one or more certificates by a certain deadline, such as those in BR section 4.9, but that deadline is not met by the CA.
- In the process of researching one incident, another incident with a distinct root cause and/or remediation is discovered.
- After an incident bug is marked resolved, the incident reoccurs.

In addition, incident bugs that involve revocation delays are now being tagged and displayed in a new section of the Incident Dashboard. Our intent is to gain a better understanding of the causes of delays and to identify potential opportunities to improve certificate agility.

F Distrust After

We have added Distrust-After capability to NSS as per bug #1465613, allowing Mozilla to distrust certificates issued after a particular 'valid from' date and chaining to a particular root without implementing custom logic as was done for the Symantec PKI deprecation. Separate dates for TLS and S/MIME distrust-after may be specified for each root cert.

Kathleen is in the process of creating a set of these changes to be made based on prior communication from CAs that have stopped issuing from one or more of their roots. CAs can send her email if they have root certs that should have these values set, such as if they are no longer issuing TLS certs in the hierarchy.

G CRLite

Significant progress has been made on the implementation of CRLite. In Firefox Nightly and Beta, CRLite is enabled and gathering telemetry but not yet used to enforce revocation checks. The timing for enabling revocation checking using CRLite has yet to be determined.

Please refer to the series of Mozilla Security Blog posts, and Thyla VanDerMerwe's presentation at the Real World Crypto conference for more information.

CRLite depends on Intermediate Preloading, in which Firefox automatically downloads the set of trusted intermediate certificates disclosed in CCADB and uses them when all certificates needed to build a chain are not sent in the TLS handshake. Intermediate Preloading is currently enabled in Firefox Nightly and Beta and is expected to be enabled in Release version 75 in April.

H TLS 1.0 and 1.1 Deprecation

Mozilla, in cooperation with Apple, Google, and Microsoft, is moving forward with plans to disable TLS 1.0 and 1.1 in March as previously announced. These versions are currently disabled in Firefox Nightly and Beta, and this change will ship in Release 74 on March 10th. For the time being, users will be shown the option to override the error. This change is being tracked in bug 1227521.