CAB Forum Guangzhou, November 2019

Browser News - Mozilla

A Intermediate Audits

Certs that are technically capable of TLS issuance must be BR audited. This has been Mozilla policy since 2013 when the BR audit requirement was introduced. Unfortunately, the recent introduction of ALV for intermediate certificates has uncovered quite a few compliance issues. One common case is intermediates that are not intended for TLS usage by the CA. These technically capable certificates must either be listed in the CA's BR audit, be revoked or expired, or be added to OneCRL. Be aware that other root programs may not accept inclusion in OneCRL as sufficient remediation.

Please proactively review your intermediate certificates for these issues and file an incident bug if non-compliance is detected. A CCADB report has been created to help identify non-compliant intermediates. This report is called "My Certs Failed Audit Letter Validation" And it is available to CAs via the 'Reports' tab in the 'CA Community Reports' folder. It is also available as a Task List item on the CCADB home page.

In the future, we plan to add ALV for EV-enabled root and intermediate certificates, so this would also be a good time to confirm that you CA certificates are properly listed in EV audit reports.

[Reference to the discussion]

B Intermediate Disclosures

We recently discovered some inconsistencies in the way that cross-certificates are disclosed. Mozilla policy requires disclosure in CCADB within one week for all cross-certificates that a CA signs.

The audit report(s) referenced in the disclosure must list the cross-certificate, just like any other intermediate CA must be listed. Those audit reports may be from the parent CA or from the CA operating (in possession of the private key of) the cross certificate. The same goes for CP/CPS disclosure: the cross-certificate must be within the scope of the policy documents that are disclosed in the CCADB record.

Rob Stradling has added two new "experimental" sections to the Mozilla disclosure report highlighting these issues:
- Disclosed, but with Inconsistent Audit details
- Disclosed, but with Inconsistent CP/CPS details

Please check these reports to ensure that the results are as expected for any of your CA certificates that are listed. For example, it is acceptable if a cross-certificate record has a different audit statement than the corresponding root certificate record as long as both audit statements exist, are current, and correctly state the certs that were in scope of the audits.

C OCSP Responses for Precertificates

A number of incidents have recently been reported relating to OCSP responses for Certificate Transparency (CT) precertificates. Mozilla currently has no technical or policy requirements for CT, but we added a "recommended practice" to clarify our expectations around precertificates. The most important points are:

- Mozilla infers from the existence of a precertificate that a corresponding certificate has been issued.
- This means that the CA must provide a valid OCSP response for a precertificate even if a corresponding certificate has not, in fact, been issued.

We would like to make this a requirement, but currently the BRs arguably prevent CAs from complying. Ballot SC23 intends to fix this issue.

D Mozilla Policy Update

I am finishing a significant Root Store Policy update covering sixteen issues in total. I strongly encourage CAs to follow along on the mozilla.dev.security.policy list and to review all of the proposed changes. It is especially important for CAs to identify policy changes that will be difficult for them to implement, or to implement in the required timeline. Unless otherwise stated, Mozilla expects CAs to comply with new policies within 1-2 months of the effective date of the new version.

Here is a rundown of the most significant proposed changes:

Beginning on 1-July, 2020, end-entity certificates MUST include an EKU extension containing KeyPurposeId(s) describing the intended usage(s) of the certificate. This requirement is driven by the issues we've had with non-TLS certificates that are technically capable of being used for TLS. Some CAs have argued that certificates not intended for TLS usage are not required to comply with TLS policies.

CP/CPS versions dated after March 2020 can't contain blank sections and must - in accordance with RFC 3647 - use "No Stipulation" to mean that no requirements are imposed. That term cannot be used to mean that the section is "Not Applicable". For example, "No Stipulation" in section 3.2.2.6 "Wildcard Domain Validation" means that the policy allows wildcard certificates to be issued.

Section 8 "Operational Changes" will apply to unconstrained subordinate CA certificates. With this change, any new unconstrained subordinate CAs that are transferred or signed for a different organization that doesn't already have control of a subordinate CA must go through a public discussion before issuing certificates.

We've seen a number of instances in which a CA has multiple policy documents and there is no clear way to determine which policies apply to which certificates. With this change, CAs must provide a way to clearly determine which CP/CPS applies to each root and intermediate certificate. This may require changes to CA's policy documents.

Mozilla already has a "required practice" that forbids delegation of email validation to 3rd parties for S/MIME certificates. With this update, we will forbid delegation of verification of the domain component in our policy.

We've also added specific S/MIME revocation requirements to policy instead of the existing unclear requirement for S/MIME certificates to follow the BR 4.9.1 revocation requirements. The new policy does not include specific requirements on the time in which S/MIME certificates must be revoked.

I've decided to defer discussion on a proposal to require newly included roots to meet all current requirements, even if the requirement wasn't in place at the time the root was created.

Other changes include:

- Clarify the Mozilla-specific requirements in ECDSA curve-hash pairs in section 5.1 (this may be delayed pending an analysis of the impact of the change on existing certificates)
- Add the P-521 exclusion in section 5.1 of the Mozilla policy to section 2.3 where we list exceptions to the BRs.
- Change references to "PITRA" in section 8 to "Point-in-TIme Audit", which is what we meant all along.
- Update required versions of audit criteria in section 3.1
- Formally require incident reporting

I am compiling all of these changes in the 2.7 branch on GitHub. My current target is for these changes to take effect in January.

E Update on Intermediate Preloading and CRLite

1. Intermediate Preloading

Our Intermediate Preloading feature consists of preloading all intermediate CAs known to the Mozilla Root Program into users' profiles. This feature is intended to resolve missing intermediate errors without the privacy compromise of AIA-fetching. We have landed this feature in Nightly, our experimental version of Firefox. We're targeting enabling this for release versions of Firefox in Q1 2020.

2. CRLite

We're making solid progress on implementing an idea that comes from academia, namely CRLite, to push all end-entity revocation information to clients. The idea makes clever use of existing information about the certificate ecosystem that comes from CT logs and

probabilistic data structures to efficiently and effectively push this information to clients. We're in the final phases of landing code for our prototype. In comparison to the academic paper, we have reduced file sizes as well as reduced revocation checking times. This technique allows clients to do revocation checking in a fast and private way. Ultimately Mozilla expects to only query OCSP responders when certificates are too young to be in the CRLite data set, or the CA's CRLs are out-of-date or unpublished.

F Distrust After

We regularly have the problem of a CA wanting to retire a root certificate by not issuing certs after a specified date, yet the existing certs are still valid for a year or more. We also have encountered scenarios in which Mozilla wants to distrust a root but doing so would have a significant impact on our users. To help with this, we've added the ability to distrust a root for all certificates issued after a certain date. This is implemented in the Mozilla root store and can be independently applied to each trust bit (Websites, Email).

G TLS 1.0 and 1.1 Deprecation

As was announced last year and I have been repeating at these meetings, Apple, Google, Microsoft, and Mozilla are coordinating to disable TLS 1.0 and 1.1 less than 6 months from now, in March 2020. TLS 1.0 and 1.1 are now disabled in Firefox Nightly. TLS 1.0 still accounts for roughly 8000 of the top 1 million websites (Tranco list). I would again like to thank the CAs who contacted their customers about this issue.