CAB Forum Cupertino, March 2019

Browser News - Mozilla

1 CCADB News

Note from Kathleen: If you updated your CA's root inclusion bug prior to February 12, and I have not responded to your update, then please send email to me. I will strive to reply to CA updates to root inclusion bugs within 4 weeks under normal circumstances, so please send email to me whenever I take longer to reply to your update.

Current Root Store Members of CCADB: Mozilla, Microsoft, Google, Cisco, Apple
(No change)

The current Audit Case workflow is described here:
https://ccadb.org/cas/updates#audit-case-workflow
(No significant changes)

Root Inclusion Cases have been redesigned to look similar to Audit Cases and have similar workflow. CAs who have access to the CCADB can now directly enter their root inclusion data as described here:
https://wiki.mozilla.org/CA/Information_Checklist
For now, CAs will continue to create a Bugzilla Bug. Then provide the "Mozilla Root Inclusion Case Information link" in the bug, and update the bug to let Kathleen know when to review the information that has been provided in the Root Inclusion Case in the CCADB.

- We plan to create tools/integration to automate this interaction between Bugzilla and CCADB.

2 Intermediate Preloading, CRLite, and CT

As we announced in London, Mozilla is doing work to cache disclosed intermediate CA certificates on the client. Initially, this will simply serve as an alternative to AIA fetching, which has never been implemented in Firefox, for misconfigured websites. Eventually, it may be used to enforce the disclosure of unconstrained intermediate CA certificates. We now have preloading running in Firefox Nightly for experimentation. More information.

Intermediate preloading is a prerequisite to the new revocation mechanism called CRLite that we also announced in London. We are continuing development work but still have no specific dates to announce.

CRLite will rely on CT logging as a means to build a complete list of issued certificates. At some point before CRLite is released, I expect to announce a list of logs that we scan to build our corpus of certificates. Mozilla's log list will certainly be similar, if not identical to Chromium's list.

Unlogged certificates can trigger false positives in CRLite. I expect our implementation to fall back to OCSP (possibly in “hard fail” mode where a problem obtaining an OCSP response results in an error) for certificates that are not delivered with an SCT from a recognized log. I also expect there to be a preference that allows users and administrators to completely disable the use of CRLite.

Mozilla has no plans to enforce CT logging at this time. We recognize the importance of CT in improving the web PKI, but the lack of a privacy-preserving mechanism to verify inclusion of a certificate in a log in real time during certificate verification is a problem that we want to solve prior to committing fully to CT. In the absence of such improvements, we view CT as a countersignature mechanism that requires trust to be placed in log operators.

3 Mozilla Policy Update

We plan to begin discussions on a series of updates to the Mozilla Root Store policy soon. The list of suggested improvements is at https://github.com/mozilla/pkipolicy/issues. Feel free to add your ideas there.

We are likely to have a discussion about requiring approval before a CA in Mozilla’s program signs a root or subordinate CA certificate that will be operated by another organization (i.e. the other organization possess the private key). We encourage CAs who currently engage in this practice to participate in that discussion.

4 Mozilla Approved Algorithms

The strict list of permitted algorithms and key sizes in section 5.1 of Mozilla policy has recently caught some CAs by surprise. Specifically, only ECDSA keys using one of the following curve-hash pairs are permitted for all certificates in the hierarchy:

- P-256 with SHA-256
- P-384 with SHA-384

This was added to the policy in 2017 and is more restrictive than the BR language. If your CA uses elliptic curves, please review your certificates for compliance. We believe that limiting the number of supported algorithms to the most common ones reduces the risk of bugs and other vulnerabilities.

5 Revocation and Incident Reporting

Mozilla recently updated the guidance for Responding to an Incident on our wiki. The revocation section now states:

Mozilla recognizes that in some exceptional circumstances, revoking misissued certificates within the prescribed deadline may cause significant harm, such as when the certificate is used in critical infrastructure and cannot be safely replaced prior to the revocation deadline. However, Mozilla does not grant exceptions to the BR revocation requirements. It is our position that your CA is ultimately responsible for deciding if the harm caused by following the requirements of BR section 4.9.1.1 outweighs the risks created by choosing not to meet this requirement.

If your CA will not be revoking the certificates within the time period required by the BRs, our expectations are that:

- *The decision and rationale for delaying revocation will be disclosed to Mozilla in the form of a preliminary incident report immediately; preferably before the BR mandated revocation deadline. The rationale must include an explanation for why the situation is exceptional. Responses similar to "we deem this misissuance not to be a security risk" are not acceptable. This rationale should be provided on a per-Subscriber basis.*
- *Any decision to not comply with the timeline specified in the Baseline Requirements must also be accompanied by a clear timeline for when the problematic certificates will be revoked and supported by the rationale to delay revocation.*
- *The issue will need to be listed as a finding in your CA's next BR audit statement.*
- *Your CA will work with your auditor (and supervisory body, as appropriate) and the Root Store(s) that your CA participates in to ensure your analysis of the risk and plan of remediation is acceptable.*
- *That you will perform an analysis to determine the factors that prevented timely revocation of the certificates, and include a set of remediation actions in the final incident report that aim to prevent future revocation delays.*

If your CA will not be revoking the problematic certificates as required by the BRs, then we recommend that you also contact the other root programs that your CA participates in to acknowledge this non-compliance and discuss what expectations their Root Programs have with respect to these certificates.

The points I would like to make are:

- We recognize that there can be situations in which revoking misissued certificates is not the best course of action
- We provide specific guidance for what CAs should do in that situation. Disclosure and learning from the incident are emphasized.
- We don't make these decisions by granting exceptions

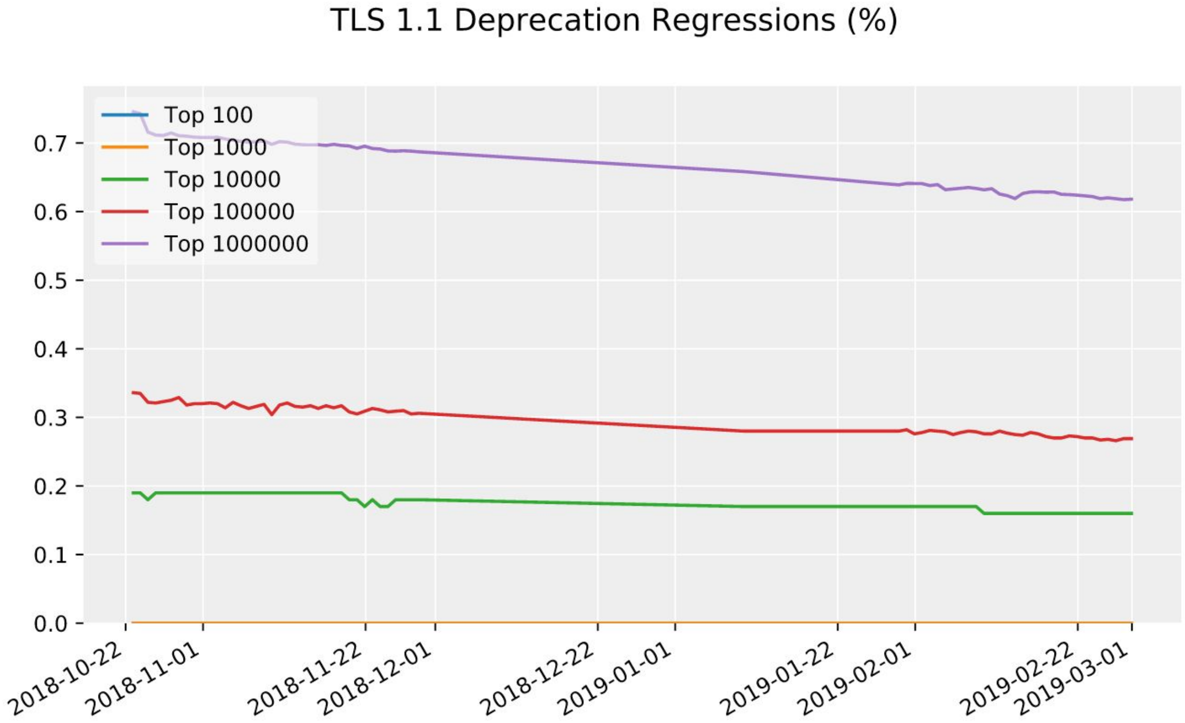
In light of the current serial number situation, I plan to update this guidance to include examples of situations where the aggregate impact is large. If you have any questions, please ask.

6 Test Certificates

A number of recent misissuances have been described as being the result of production testing. We do understand that post-production testing can be an important component of a test plan, and our intent is not to discourage the thoughtful use of this tool. However, please be aware that there is no testing exception for certificates issued from a publicly-trusted hierarchy. Pre-certificates issued for testing purposes must be fully vetted and treated no differently than any other certificate in a publicly-trusted hierarchy. Testing is not an acceptable reason for failing to report misissuance.

7 TLS 1.0 and 1.1 Deprecation

As was announced last year, Apple, Google, Microsoft, and Mozilla are coordinating to disable TLS 1.0 and 1.1 one year from now, in March 2020. TLS 1.0 still accounts for roughly 1% of connections and 0.7% of the top 1 million websites (graph below) in Firefox. We could use CAs help in getting the word out about this change. One suggestion is for CAs to notify their customers whose servers don't yet support TLS 1.2 during the renewal process. This would be a great service to those customers and the internet as a whole.


TLS 1.1 Deprecation Regressions (%)
Top 100
Top 1000
Top 10000
Top 100000
Top 1000000