EJBCA Security Advisory - Validities not calculated per RFC 5280

2020-10-23 - Rubina Akram - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - Validities not calculated per RFC 5280

Dear Customers and Partners,

PrimeKey has released an update to address a compliance issue, as reported to us by a customer.

Issue Summary

This mail affects those of you required to conform to requirements of CA/Browser-Forum and the various browser root programs. We have been alerted to the fact that EJBCA in versions prior to version 7.4.3 does not calculate validity times in conformance to the Baseline Requirements version 1.7.1 and later. The baseline requirements since then specify that validity for certificates and OCSP responses is "For Certificates issued on or after 2020-09-01, the validity period is as defined within RFC 5280, Section 4.1.2.5: the period of time from notBefore through notAfter, inclusive."

What this implies is that a certificate with a validity defined as 1 day in EJBCA would be exactly 86400 seconds, including the second noted in the notBefore field, while RFC 5280 specifies the gap between notBefore and notAfter to be 23 hours, 59 minutes and 59 seconds. In other words, according to the RFC certificates and OCSP responses produced though EJBCA have a validity of one second more than intended. This will be been amended since EJBCA version 7.4.3 to be in line with the RFC.

How to check if you are affected?

The baseline requirements and root programs require that no certificate

have a validity time of more than 398 days, which according to the definition above means 397 days, 23 hours, 59 minutes and 59 seconds between the times defined in notBefore and notAfter. If you have, since 2020-09-01, issued certificates with a validity time specified as 398 days in EJBCA you are going to be required by the root programs to revoke those certificates within five days of being alerted, since those certificates will have a validity of one second too long. Any certificates with a validity of 397 days or shorter are still within requirements, thus this issue only affects you if you have configured the validity to exactly 398 days in EJBCA.

Mitigation

If unsure, please verify that certificate and OCSP validity times are well within the threshold required by the baseline requirements.

Fixes

EJBCA 7.4.3 will be released within the next few weeks on all platforms which addresses this issue and will calculate validities in accordance with the RFC.

We will in a weeks time also post this information as an incident report on mozilla.dev.security.policy

If you have any questions, please contact support.