EJBCA Security Advisory - Domain Security over EST

2020-11-05 - Mike Agrenius Kushner - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - Domain Security over EST

Dear Customers and Partners,

PrimeKey has released an update to address a vulnerability in EJBCA found as a part of our internal testing.

As a part of PrimeKey's new policy, we will be submitting this issue publicly as a CVE two weeks after alerting customers

Issue Summary

A security issue was found when enrolling with EST while proxied through an RA over the Peers protocol. As a part of EJBCA's domain security model, the peer connector allows the restriction of client certificates (for the RA, not the end user) to a limited set of allowed CAs, thus restricting the accessibility of that RA to the rights it has within a specific role. While this works for other protocols such as CMP, it was found that the EJBCA enrollment over EST implementation bypasses this check, allowing enrollment with a valid client certificate through any functioning and authenticated RA connected to the CA.

Who is potentially affected

You may be affected if you are using EST over RAs connected to Peers and they are split into separate domains.

Who is not affected

You are not affected by this advisory if you are not using EST or using EST but without multi tenancy.

Severity

PrimeKey rates the issue as having medium impact and low probability.

Risk Assessment

Impact is medium as it would allow a trusted client on one RA to enroll for certificates over another RA which does not have authorization for that CA. The client still needs its own authorization to that specific CA though.

Vulnerability

You may be affected if you are using EST over RAs connected to Peers and they are split into separate domains.

For an exploit to be successful, the already need to have a trusted client certificate and authorization to enroll against the targeted CA - it can now do so over another RA which is not itself authorized for operate against that CA.

How to check if you are affected

If there is any risk that this may have been exploited, please review your audit logs for any incorrect issuances.

Fixes

A software update has been released in EJBCA Enterprise 7.4.3.

For more information, see the release notes included in the documentation for this release.

EJBCA 7.4.3 is included in Appliance version 3.5.5 and EJBCA Cloud 2.5.

If you have any questions, please contact support.