EJBCA Security Advisory - Enrollment Secrets Logged in Audit Log

2021-08-16 - Mike Agrenius Kushner - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - Enrollment Secrets Logged in Audit Log

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

When audit logging changes to the alias configurations of various protocols that use an enrollment secret, any modifications to the secret were logged in cleartext in the audit log.

Who is potentially affected

You may be affected if you are running any of the following protocols: SCEP, CMP or EST.

Severity

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

Risk Assessment

Impact is low as an attacker would already need to be a trusted administrator with access to the audit log.

Vulnerability

You may be affected if you are using SCEP, CMP or EST.

How to check if you are affected

Verify in the audit logs that no unauthorized issuances have been made. If there is any suspicion that a hostile party has had access to the Audit Log, change the enrollment secrets after upgrading.

Fixes

A software update has been released in EJBCA Enterprise 7.6.0.

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

EJBCA 7.6.0 is included in Appliance version 3.8.0 and EJBCA Cloud 2.7.0

If you have any questions, please contact support.