EJBCA Security Advisory - XSS and CSRF Issues

2020-03-23 - Mike Agrenius Kushner - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - XSS and CSRF Issues

Dear Customers and Partners,

PrimeKey has released an update to address two XSS issues and a CSRF issue. We would like to thank Matthias Kaiser of Apple Information Security for reporting this issue.

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

Two Cross Side Scripting (XSS) vulnerabilities have been found in the Public Web and the Certificate/CRL download servlets, and one with Cross Site Request Forgery (CSRF) issue has been found in the CA UI.

Who is potentially affected

All EJBCA installations are affected.

Severity

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

Risk Assessment

As is common with XSS and CSRF vulnerabilities generally, risk is associated with a malicious administrator or an administrator following links to pages within EJBCA sent from a malicious source, both of which are unlikely within a secure environment.

The CSRF issue could by a talented attacker, with knowledge about the CA system and network access to it, be used for privilege escalation.

How to check if you are affected

All recent versions of EJBCA are affected.

Fixes

A software update has been released in EJBCA Enterprise 6.15.2.6 and 7.3.1.2.

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

EJBCA 7.3.1.2 is included in Appliance version 3.4.5 and EJBCA Cloud 2.0.

If you have any questions, please contact support