EJBCA Security Advisory - Authentication Bypass Vulnerability

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

EJBCA Security Advisory - Unchecked Certificate Uploads in Validator

Dear Customers and Partners,

PrimeKey has released an update to address a critical vulnerability. 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 Description

During penetration testing it has been found that an error state can be generated in the CA UI by a malicious user, which in turn allows exploit of other bugs, which can lead to privilege escalation and remote code execution.

Who is potentially affected

All customers using the CA UI.

Who is not affected

If the CA UI is not accessible on a port that does not require client certificate authentication (port 8442 or 8080 on a standard EJBCA installation), the vulnerability can not be exploited.

Users of the PrimeKey PKI Appliance are **not** affected as the PKI Appliance by default implements firewall rules as described in the mitigation section.

Severity

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

Risk Assessment

The consequences of this bug being exploited are severe.

Vulnerability

This vulnerability affects all systems with the CA UI enabled.

Mitigation

We recommend the following configuration measures to assure not to be affected:

1. Use a firewall to ensure that the CA UI URI can only be accessible using client certificate authentication.
2. Verify (as best you can) that no nodes have been compromised by checking audit logs for unauthorized access.

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.