EJBCA Security Advisory - Protocol Access Control Bypass

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

EJBCA Security Advisory - Protocol Access Control Bypass

Dear Customers and Partners,

PrimeKey has released an update to address a vulnerability in EJBCA's modular access control. 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

EJBCA allows the restriction of available remote protocols (CMP, ACME, REST, etc) through the system configuration. A vulnerability where these restrictions can be bypassed by modifying the URI string from a client.

EJBCA's internal access control restrictions are still in place, and each respective protocol must be configured to allow for enrollment.

Who is potentially affected

You may be affected if you PKI is set up for enrollment over a 3rd party protocol, but have for whatever reason disabled that protocol in the System Configuration.

Who is not affected

You are not affected by this advisory if you have not configured any protocols or if using them have not disabled any of them.

Severity

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

Risk Assessment

PrimeKey estimates the risk of this vulnerability to be low. The use case of having a protocol fully configured yet disabled is uncommon, and even if protocol access is restricted internal access controls are still in place.

Vulnerability

This vulnerability can only affect a system that has a remote enrollment protocol configured yet disabled.

How to check if you are affected

Check if aliases exist for EST, SCEP, CMP or ACME under their respective configuration screens, then verify if any of those with aliases are disabled under the System Configuration screen.

If so, check with the audit logs if any certificates have been issued according to those aliases for the period when the respective protocol was supposed to be disabled.

Mitigation

As we assess the impact of this issue to be low, we do not specifically recommend that any measures be taken to mitigate it prior to upgrading EJBCA.

That said, to ensure complete mitigation of this vulnerability we recommend that you block access paths to unwanted protocols (e.g ejbca/publicweb/cmp) in your firewall.

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.