EJBCA Security Advisory - Unchecked Certificate Uploads in Validator

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 minor bug. 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

During testing it has been found that the External Command Certificate Validator, which allows administrators to upload external linters to validate certificates, saves uploaded test certificates to the server. An attacker who has gained access to the CA UI could exploit this to upload malicious scripts to the server.

Who is potentially affected

You may be affected if you use the External Command Certificate Validator.

Who is not affected

You are not affected by this advisory if you do not use the External Command Certificate Validator.

Severity

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

Risk Assessment

Risks associated with this issue alone are negligible unless a malicious user already has gained access to the CA UI through other means, as a trusted user is already trusted to upload scripts by virtue of having access to the validator.

An attacker must first have gotten access to the CA environment, which is presumably in a secure zone.

Vulnerability

For an exploit to be successful, several factors are required:

1. An attacker must have bypassed access control checks and given themselves full access to the CA UI.

If these conditions are met, then an attacker may use this exploit in a chain of others in order to gain control of the PKI.

How to check if you are affected

Check audit logs for discrepancies in the audit log, specifically unplanned access of the validator pages or any certificates issued without provenance.

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