EJBCA Security Advisory - Deserialization Bug

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

EJBCA Security Advisory - Deserialization Bug

Dear Customers and Partners,

PrimeKey has released an update to address a vulnerability in EJBCA. 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

Several vulnerable sections of code were found, where the verification of serialized objects sent between nodes connected via the Peers protocol still allows unsecure objects to be deserialized.

Who is potentially affected

You may be affected if you have connected your VAs or RAs via the Peers protocol.

Who is not affected

You are not affected by this advisory if you are not using the Peers protocol.

Severity

PrimeKey rates the issue as having high impact by low probability.

Risk Assessment

Impact is high as it would allow malicious code execution, but probability as low as it would require severe compromise of the internal PKI infrastructure beforehand.

Vulnerability

This vulnerability can only affect a system that has EJBCA nodes connected via the Peers protocol.

For an exploit to be successful, an attacker needs to have compromised the internal PKI in order to issue fraudulent TLS keys.

or

An attacker must have performed a complete takeover of one of the nodes in order to send a compromised payload.

If these conditions are met, then an attacked could inject and execute malicious code on the CA.

How to check if you are affected

On the CA, enter the CA UI and verify if you have any VAs or RAs connected over the Peers protocol on the Peer Systems view.

Mitigation

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

1. Verify audit logs and keys that TLS has not been compromised within your network
2. Verify (as best you can) that no nodes have been compromised by checking system logs for unauthorized access or unexpected application server reboots.

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.