EJBCA Security Advisory

2019-12-02 - Pamela Kiewitt - Comments (0) - PrimeKey Announcements

EJBCA Security Advisory

Dear customers and partners,

PrimeKey has released an update to address a privilege assignment issue, discovered during PrimeKey's internal development and security process.

Privilege Assignment

The assignment issue opens for the possibility to issue certificates from CAs other than the one configured when using SCEP in RA Mode.

Who is potentially affected

You may be affected only if you are using SCEP in RA mode.

Who is not affected

If you are not using SCEP in RA mode, then you are not affected by this advisory.

Severity

PrimeKey rates the issue as having a potentially high impact but low probability.

Risk Assessment

The issue is due to a logic flaw in the implementation of how a SCEP Alias configured in RA mode handles which CA is requested by the client when the client is an authenticated RA.

Potentially, the issue would allow a remote authenticated RA with access to a SCEP RA alias to issue certificates from any CA in the system, not only the CA configured as RA CA Name in the SCEP alias.

Vulnerability

This vulnerability can only affect a system that has an active SCEP alias configured in Operational mode: RA.

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

1. The client is an authenticated SCEP RA (using an RA authentication password).

2. The certificate profile and the end entity profile configured in the SCEP alias allow access to other CAs, in addition to the CA configured as **RA CA Name**.

If these conditions are met, then the authenticated RA could get certificates issued from other CAs, which are available in the certificate- and end entity profiles.

How to check if you are affected

To verify if a SCEP alias is configured in RA Mode, do the following:

Open the EJBCA Admin UI and select **SCEP Configuration.**

- If the List of SCEP Aliases is neither empty nor does the **Mode** column contain **RA**, you are not affected.

If you have a SCEP Alias configured in “RA Mode”, click the Alias name to view the configuration:

For the end entity profile selected as **RA End Entity Profile**:

- Click the EJBCA Admin UI menu option **End Entity Profiles**, select the profile and then click **Edit End Entity Profile**.

- Scroll down to **Available CAs** and verify that only desired CAs are selected.

If not, go to mitigation

For the certificate profile selected as **RA Certificate Profile:**

- Click the EJBCA Admin UI menu option **End Entity Profiles**, select the profile and then click **View**.

- Scroll down to **Available CAs** and verify that only desired CAs are selected.

If not, go to mitigation.

You are not affected:

If no SCEP Alias configured in RA mode is available.If you see only desired CAs as selected

in certificate- and end entity profiles.

Mitigation

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

- In your present SCEP RA Alias configuration, edit the certificate- and end entity profiles to only select desired CAs as **Available CAs** (ensuring that **Any CA** is not selected).

- If you must have **Any CA** selected, we strongly recommend upgrading to one of the maintenance release listed below.

Fixes

A software update, ensuring that only the CA configured as **RA CA Name** can be used, has been released in **EJBCA Enterprise 7.3.1.1** and **6.15.2.5.**

For more information, see the EJBCA 7.3.1.1 Release Notes Link: https://doc.primekey.com/x/uhOK and EJBCA 6.15.2.5 Release Notes Link: https://doc.primekey.com/x/wROK.

EJBCA 7.3.1.1 is included in Appliance version 3.4.3 Link: https://doc.primekey.com/x/loG8 and EJBCA Cloud 1.18.1 Link: https://doc.primekey.com/x/DIC8.

If you have any questions, please contact support.