EJBCA Security Advisory - Vulnerability in Apache Batik

2021-02-08 - Mike Agrenius Kushner - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - Vulnerability in Apache Batik

Dear Customers and Partners,

PrimeKey has released an update to address a CVE reported to one of EJBCA's underlying libraries, Apache Batik, which may constitute a security vulnerability.

Issue Summary

CVE-2019-17566 has been reported for Apache Batik, which constitutes an exploitable vulnerability for EJBCA. EJBCA 7.4.3.2 includes an upgrade of this library to version 1.13, and as this constitutes a vulnerability in EJBCA we will be submitting our own CVE two weeks after the release of this version. The issue in the batik library makes it possible to make the server (where batik is used (JBoss/WildFly)) to make an outgoing HTTP GET request.

The library is only used for the function "Printing of user data" in End Entity Profiles, where the library is used to parse an SVG print template uploaded to EJBCA. The issue is triggered when uploading a new SVG template when editing an end entity profile. This functionality is rarely used.

In addition to this, CVE-2020-26217 has been reported for the XStream library as well. While the vulnerability in this library does not constitute a security risk for EJBCA, it has been upgraded as well.

Who can access the functionality:

This functionality is only available to trusted administrators with access to Edit End Entity Profile. Access rules that must be enabled to access this functionality:

/ra_functionality/edit_end_entity_profiles/

Authentication needed to access this functionality:
Client Certificate authentication to EJBCA CA UI

How to check if you are affected

This affects all current versions of EJBCA up until EJBCA 7.4.3.2

Related audit log records:
Whenever an End Entity Profile is edited, an audit record is created with information what was edited, and by which, strongly authenticated, administrator.

Related log records:
15:24:40,419 INFO [org.cesecore.audit.impl.log4j.Log4jDevice] (default task-4) 15:24:40+01:00;RA_EDITEEPROFILE;SUCCESS;RA;EJBCA;CN=SuperAdmin;;;;msg=End entity profile aaaa
edited.;changed:PRINTINGSVGDATA=PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9

It is thus possible to see in the audit log if SVG templates have been uploaded by the fact that the field PRINTINGSVGDATA was checked in an RA_EDITEEPROFILE event.

Mitigating factors

Only strongly authenticated administrators with high privileges are able to access this functionality.
Causing the server to perform outgoing HTTP requests does not in itself constitute a breach.

Other mitigations:
As the issue in the batik library makes it possible to make the server (JBoss/WildFly) to make an outgoing HTTP GET request. EJBCA normally does not rely on making outgoing http connections for it's functionality, except for specific functionality that is no enabled by default. Such requests can thus be limited to not be allowed to be performed by the CA server to untrusted networks, to other servers than needed (such as for example CT log servers).

Fixes

EJBCA 7.4.3.2 has been released on all platforms. Upgrading EJBCA will resolve this vulnerability. As per our standard policy, PrimeKey will register this issue as a CVE on EJBCA two weeks after posting this article.

Best regards,

The PrimeKey Team