



Portal > > PrimeKey Announcements > EJBCA Security Advisory - General Purpose Custom Publisher able to Run Despite External Scripts Being Disabled

EJBCA Security Advisory - General Purpose Custom Publisher able to Run Despite External Scripts Being Disabled

2021-08-16 - Mike Agrenius Kushner - 0 Comments - in PrimeKey Announcements

EJBCA Security Advisory - General Purpose Custom Publisher able to Run Despite External Scripts Being Disabled

Dear Customers and Partners,

PrimeKey has released an update to address a vulnerability in EJBCA found as a part of our internal testing.

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

It was found during testing that the General Purpose Custom Publisher, which is normally run to invoke a local script upon a publishing operation, was still able to run if the System Configuration setting **Enable External Script Access** was disabled. With this setting disabled it's not possible to create new such publishers, but existing publishers would continue to run.

Who is potentially affected

You may be affected if you have a General Purpose Custom Publisher existent and active, but expect it to be disabled due to external scripts being disabled in the System Configuration.

Severity

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

Risk Assessment

While it would be possible for an attacker to have operating system scripts running with the knowledge of a PKI administrator, the existence of the prerequisite publisher and it being active in spite of external scripts being disabled is unlikely, an attacker would also need to

have operating system privileges in order to exploit such an attack.

Vulnerability

You may be affected if you have a General Purpose Custom Publisher existent and active, but expect it to be disabled due to external scripts being disabled in the System Configuration.

How to check if you are affected

Verify that no such publisher exists, and if it does that it's functioning as expected, i.e. that you have not assumed that it would be inactive due to external scripts being disabled.

Fixes

A software update has been released in EJBCA Enterprise 7.6.0.

For more information, see the release notes included in the documentation for this release.

EJBCA 7.6.0 is included in Appliance version 3.8.0 and EJBCA Cloud 2.7.0

If you have any questions, please contact support.