Regarding key blacklist entries

2020-03-13 - Pamela Kiewitt - 0 Comments - in PrimeKey Announcements

EJBCA comes with a feature called "Public Key Blacklist Validator". If used, this blacklist holds hashes of public keys for which a CA should not be allowed to issue certificates. The blacklist is empty by default and is filled with key hashes using a CLI command.

Background

There was a bug in OpenSSL (CVE-2008-0166) [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166] where a vulnerable version of the library used only the PID as seed when generating RSA or DSA keys, allowing an attacker to find the private key from the corresponding public key without much effort.

This buggy version of OpenSSL was distributed in two Debian packages between 17th of September 2006 and 13th of May 2008.

The blacklist feature in EJBCA is commonly used to prevent issuance of certificates containing keys created with the buggy version of OpenSSL.

Incomplete Lists

PrimeKey has previously provided customers, as a courtesy, with a blacklist of weak keys as created by the Metasploit project.

It has been brought to our attention that the list from the Metasploit project was not complete. More complete blacklists were created by Debian maintainers, but those lists are not directly usable by the EJBCA blacklist feature.

Solution

We have documented how to use instead an "External Command Certificate Validator" to verify a certificate against the Debian blacklists.

If mandated to check for weak Debian keys we recommend not to rely on the Metasploit blacklist, but instead:

- Update your blacklist database and verify that the database has all the entries you require

Or

- Use an "External Command Certificate Validator" to verify certificates against the Debian blacklists before issuance.

From our documentation:

Key Validators:

https://doc.primekey.com/ejbca/ejbca-operations/ejbca-ca-concept-guide/validators-overview/key-validators

Post Processing Validators:

https://doc.primekey.com/ejbca/ejbca-operations/ejbca-ca-concept-guide/validators-overview/post-processing-validators

The external command certificate validator can be found in this section:

https://doc.primekey.com/ejbca/ejbca-operations/ejbca-ca-concept-guide/validators-overview/post-processing-validators#PostProcessingValidators-DebianWeakKeyChecks