SecurityServer Advisory for CVE-2018-19589 PKCS#11 R2 Security Officer Rights

Utimaco has been made aware of a vulnerability affecting the PKCS#11 R2 provider shipped with our SecurityServer product package.

1 Issue

1.1 Description

When successfully authenticated as Security Officer (SO) to a PKCS#11 slot for which external key storage has been configured, this SO can retrieve attributes of keys marked as private keys, and delete keys marked as private keys. The availability of external keys marked as private may thus be compromised; the confidentiality and integrity of such keys is not compromised.

1.2 Issue ID

Internal issue ID HSM-5258. This issue has been filed in the Common Vulnerabilities and Exposures list as CVE-2018-19589, see https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2018-19589

1.3 Detailed description

The PKCS#11 base specification[1] (section 4.4) defines that “When the CKA_PRIVATE attribute is CK_TRUE, a user may not access the object until the user has been authenticated to the token.” The PKCS#11 Usage Guide[2] (section 2.4) states more precisely that “This version of Cryptoki recognizes two token user types. One type is a Security Officer (SO). The other type is the normal user. Only the normal user is allowed access to private objects on the token, and that access is granted only after the normal user has been authenticated.”.

Notice: In the sense of the PKCS#11 specification, the private part of an asymmetric key may have the CKA_PRIVATE attribute set to CK_FALSE, and the public part of an asymmetric key may have the CKA_PRIVATE attribute set to CK_TRUE. The vulnerability described in this advisory applies to the term “private” in the PKCS#11 sense, i.e. to keys which have their attribute CKA_PRIVATE set to CK_TRUE.

[1] PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 Plus Errata 01, 13 May 2016, OASIS
[2] PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40, 16 November 2014, OASIS

SecurityServer Advisory for CVE-2018-19589 PKCS#11 R2 Security Officer Rights

A Security Officer who has successfully authenticated to the CryptoServer HSM can a) see and retrieve attributes of keys in the external key store which are marked as private keys, i.e. which have their CKA_PRIVATE attribute set to CK_TRUE, and b) delete such keys marked private. An authenticated SO can thus accidentally or maliciously compromise the availability of keys marked private.

The SO is not able to see or retrieve the actual key value; modify the key value or any key attribute; use the key for any key usage it is foreseen for, i.e. cannot sign, encrypt, derive other key material using this key; etc. The confidentiality and integrity of keys marked private is thus not compromised.

The vulnerability only affects keys for which external key storage has been configured, i.e. where keys are stored as encrypted and integrity-protected key blobs outside the HSM. Keys stored inside the HSM are not affected, i.e. an authenticated SO can neither see nor delete keys marked as private when they are stored inside the HSM.

1.4 Affected Utimaco product(s), component(s) and version(s)

- CryptoServer PKCS#11 R2 library ‘cs_pkcs11_R2’ for Windows and Linux, version 2.31 and above, shipped with SecurityServer 4.00.and above
- Command-line administration tool ‘p11tool2’ for Windows and Linux, version 2.0.3 and above, shipped with SecurityServer 4.00 and above
- CryptoServer SDK customers may be affected when using the CryptoServer SDK to implement PKCS#11 Vendor Defined Mechanisms.

As mentioned before, the vulnerability affects the components above only when using external key storage. Affected components are not vulnerable when using internal key storage, i.e. when storing PKCS#11 keys inside the HSM.

1.5 Not affected Utimaco product(s), component(s) and version(s)

- SecurityServer components:
  - Graphical administration tool for the PKCS#11 provider ‘P11CAT’. Although P11CAT includes the vulnerable PKCS#11 library, the way P11CAT uses the PKCS#11 library functions inhibits the exploit of this vulnerability.
  - Cryptographic provider other than the PKCS#11 provider, i.e. CSP/CNG provider, JCE provider.
  - Administration tools for cryptographic provider other than the PKCS#11 provider, i.e. ‘cxitool’, ‘cngtool’, ‘csptool’, ‘KeyCAT’.
  - HSM administration tools ‘csadm’, ‘CAT’.
- SecurityServer’s former PKCS#11 R1 provider
- CryptoServer CP5, TimestampServer, PaymentServer, CryptoScript SDK

SecurityServer Advisory for CVE-2018-19589 PKCS#11 R2 Security Officer Rights

2 What To Do

Please follow the instructions below if you are operating an affected component and use external key storage for storing your PKCS#11 keys. In case you use internal key storage, you are not affected and thus don't need to take any action.

Utimaco has released patch HSM-5258 for the CryptoServer PKCS#11 R2 implementation, which includes new versions of the following components

- PKCS#11library cs_pkcs11_R2.dll (Windows) resp. cs_pkcs11_R2.so (Linux)
- Command line administration tool p11tool2, linked with the new PKCS#11 R2 library
- Graphical administration tool P11CAT, linked with the new PKCS#11 R2 library

This patch is available in our support portal under Support -> Downloads -> SecurityServer Se Gen2 and Support -> Downloads -> SecurityServer CSe. Login to the support portal is required.

Please notice: This patch requires minimum HSM firmware as per SecurityServer 4.01.0. In case you are running HSM firmware prior SecurityServer 4.01.0, you should first download the SecurityServer 4.01.0 Product CD or a more recent Product CD from our support portal, install this Product CD, and only then apply the patch as described in the next section. Please consult the SecurityServer 4.01.0 Release Notes to retrieve the firmware module versions for SecurityServer 4.01.0, and check whether your operational firmware is equal or superior to these versions.

When operating the CryptoServer PKCS#11 provider with external key store, you should retrieve patch HSM-5258.zip from our support portal, extract the respective library and tools for your Operating System (Windows or Linux, 64 bit or 32 bit version) and overwrite the vulnerable components in the installation directory.

Whether you are affected by this vulnerability or not, we recommend that you follow best practices for physical and logical access control, and limit access to the PKCS#11 configuration file and the PKCS#11 external key storage to authorized persons and applications.

If you need more information or guidance, please contact our technical support as well.

SecurityServer Advisory for CVE-2018-19589 PKCS#11 R2 Security Officer Rights

3 Technical support

You can find technical support for Utimaco products in any of these ways:

Download product information from https://hsm.utimaco.com/cryptoserver/ .

Contact us at http://hsm.utimaco.com/contact/ .

Send an email to support-cs@utimaco.com , including your hardware serial number(s), software version number(s), operating system(s) and patch level(s), and the text of any error messages.

Contact our support hotline: EMEA and Asia +49 241 1696 155, Americas +1-844-UTIMACO

4 Legal notices