utimaco®

Utimaco IS GmbH • Germanusstraße 4 • 52080 Aachen

To whom it may concern

05.10.2015

CVE-2015-6924 Elliptic Curve key disclosure vulnerability

Utimaco has been informed by Dennis Felsch and Juraj Somorovský, researchers at Horst Görtz Institute for IT-Security, Ruhr-University Bochum, about a vulnerability affecting Utimaco's product package "SecurityServer". It allows an authenticated user to disclose a secret Elliptic Curve (EC) key stored inside an Utimaco HSM.
This vulnerability has been filed under ID CVE-2015-6924 in the "Common Vulnerabilities and Exposures" list.

The vulnerability

Up to and including SecurityServer 3.21.0 an attacker performing numerous Elliptic Curve key agreements with specially selected EC public keys as input data, may retrieve partial information about the EC secret key stored inside the HSM; post-processing this information allows him to disclose the value of this EC secret key.

Which keys are affected?

Only Elliptic Curve keys for which the key usage attribute "Derive" is set, i.e. EC keys which can be used for key derivation and key agreement, are affected. An Elliptic Curve key which shall be used for ECDSA signing operations but has the "Derive" key usage attribute set, is also affected.
An Elliptic Curve key which shall be used for ECDSA signing operations and does not have the "Derive" key usage attribute set, is not affected. RSA, AES, DES and other keys are not affected at all.

Who can exploit this vulnerability?

Execution of the key agreement function requires successful authentication by an individual respectively an application using an active "cryptographic user" user account. For exploiting the vulnerability an attacker must thus either be an insider or have been able to steal valid credentials of an authorized cryptographic user. An intruder without valid authentication credentials cannot exploit this vulnerability.

Is the operational state of my HSM affected?
No, the vulnerability does neither have an impact on the operational state nor on the performance of your HSM. Keys and data stored inside the HSM, and firmware executing inside the HSM, can neither be modified nor deleted through this vulnerability.

Has there been a successful exploit?
Besides a proof of concept by Felsch & Somorovský, no exploit is known as of today.

Has this vulnerability been fixed?
This vulnerability is fixed in version 1.1.5.2 of Utimaco's firmware module ECA, where more stringent checks on the EC public key given as input for an EC key agreement handshake are performed. The ECA module 1.1.5.2 is part of the recently released product package SecurityServer 3.30.0.

How can I repair this vulnerability?
If you have a valid maintenance contract, please logon to the Utimaco Portal, download and install the SecurityServer 3.30.0 product CD, and load the SecurityServer 3.30.0 firmware package into your HSM(s).
If you have not purchased maintenance, contact our support for receiving the ECA firmware module 1.1.5.2, and instructions for installation of this firmware module.

Should I take additional measures?
Utimaco strongly encourages all users of our Hardware Security Modules to take the following measures as part of their security policy.

- Do not rely on default settings for key usage attributes. Instead, explicitly disable non-intended key usage. Would the attribute "Derive" have been disabled, it would have thwarted this specific vulnerability.
- Set key usage attributes already during key generation or import, and avoid "adjusting" attributes at a later point in time.
- In general, limit the allowed usage of a key to only those mechanism(s) the key shall actually be used for. Disable key usage attributes such as "Encrypt", "Derive", "Sign" etc. if a key is not foreseen to be used for encryption, key derivation and key agreement, signing, etc.
- Disallow modification of key usage attributes by disabling the "Modifiable" property of a key. Ensure that all key usage attributes have been enabled resp. disabled as intended prior to disabling the "Modifiable" property; once "Modifiable" has been disabled, key usage attributes cannot be changed anymore.
- Apply state-of-the-art active security mechanisms to your application host, including, but not limited to, virus scanners and intrusion detection systems.
- Always keep user credentials confidential. Whenever possible, avoid storing authentication passwords in configuration files.

In case you have further questions about this vulnerability, visit https://support.hsm.utimaco.com/support/contact to find email addresses and phone numbers for contacting our support team.

With best regards
Utimaco IS GmbH