Security Bulletin

Entrust Datacard Security Bulletin E17-006

Vulnerability of RSA Keys Generated by Some Infineon Security Modules (CVE-2017-15361)

October 20, 2017

Who should read this bulletin:

Customers using smart cards, TPMs, or other devices that contain a security module manufactured by Infineon.

Summary:

Recently, a team of researchers discovered CVE-2017-15361 (ROCA), a weakness in the RSA key generation algorithm used in some Infineon security modules. As a result, given access to an RSA public key generated by an affected module, it is possible to determine the corresponding private key using a moderate amount of computing resources. Entrust Datacard products may be used in conjunction with affected hardware. Entrust Datacard urges customers to identify hardware-based cryptographic modules in their environment and ensure that affected devices are patched and any RSA key pairs generated by them are replaced.

Impact of Vulnerability:

Security Modules

The ROCA vulnerability affects only certain security modules manufactured by Infineon. Entrust Datacard has confirmed that the Entrust Datacard SC100 and SC200 series smart cards and USB100 and USB200 tokens are not affected. Also, Gemalto has confirmed that the following tokens and smart cards are not affected:

- eToken 7300
- eToken 5110 (FIPS and non-FIPS)
- eToken 5100
- IDPrime MD 830 Rev B cards
- IDPrime PIV 2.0 cards

The Gemalto Hardware Security Modules Luna SA 4 through 7 and Protect Server are also not affected.

RSA key pairs generated in software with an Entrust Datacard security toolkit are not affected.

Many Entrust Datacard products include support for arbitrary cryptographic tokens such as smart cards and TPM-backed virtual smart cards through generic interfaces such as PKCS #11 and CAPI. These devices and the keys generated by them could be affected if they contain an Infineon security module. Customers are encouraged to test these cryptographic tokens and to patch affected devices and replace any affected RSA key pairs as described in the Corrective Action section below.

Publicly Trusted SSL Certificates

Entrust Datacard has tested all Entrust Datacard SSL certificates issued to customers prior to October 10, 2017 that were not expired as of that date; none were found to be affected by the ROCA vulnerability.

Other Potential Entrust Datacard Product Impact

Entrust Authority Security Manager may have been used to issue certificates containing vulnerable RSA keys generated by an affected security module. Also, a number of Entrust Datacard products can be configured to trust certificates containing vulnerable keys. Affected certificates should be revoked as described in the Corrective Action section below.

Mitigating Factors:

- Encryption keys are often generated on the server side and imported into the cryptographic module. Only keys generated by a vulnerable security module are affected, so encryption keys are less likely to be affected than signing keys.
- The RSA key generation algorithms implemented in Entrust Datacard toolkits are not affected by this vulnerability.
- There are no known cases involving the exploitation of this vulnerability among Entrust Datacard's customers.

Corrective Action:

Customers are encouraged to contact the suppliers of their cryptographic devices to determine if they are affected. Generated public keys can also be tested using one of the detection tools made available by the ROCA research team. Affected devices should be patched or replaced, and affected RSA key pairs revoked and replaced.

While RSA key pairs generated by Entrust Authority Security Manager itself are not affected, Entrust Authority Security Manager may have been used to issue certificates containing affected RSA public keys generated by an affected security module. These certificates should be revoked using Entrust Authority Security Manager Administration or Administration Services.

In a number of Entrust Datacard products, it is possible to import certificates from external sources. Customers concerned that an affected security module may have generated the RSA public key in imported certificates are encouraged to contact the security device vendor to determine if it is affected, and to test the potentially affected RSA keys using the tools mentioned earlier. Any certificates containing vulnerable keys should be removed from the product.

Support:

Entrust Datacard customer support is available by phone at our regular support numbers.