Infineon RSA library does not properly generate RSA key pairs

**Bullet Number** - [20171018]
**Issue Date**: Oct 19, 2017

**References:**
CERT.org : [http://www.kb.cert.org/vuls/id/307015](http://www.kb.cert.org/vuls/id/307015)
CVE-2017-15361, commonly referred to as ROCA: [https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361)

**Severity Level**: Severity varies depending on product usage.

**Background**

Infineon has reported that the Infineon RSA library version 1.02.013 does not properly generate RSA key pairs, which may allow an attacker to recover the RSA private key corresponding to an RSA public key generated by this onboard cryptographic software library. Note that Infineon reports the vulnerability does not affect the chip itself. In addition, for additional information on the industry-wide impact, refer to the following link sponsored by the US Department of Homeland Security: [http://www.kb.cert.org/vuls/id/307015](http://www.kb.cert.org/vuls/id/307015)

This vulnerability does not affect generally available Gemalto Enterprise & Cybersecurity (E&C) products. However, Gemalto security teams have assessed the portfolio of supported Gemalto products and found that the IDPrime .NET product series, which are in “end-of-sale” status, make use of the affected Infineon software library. As such, this product family may be affected when the on-board RSA key generation feature is used. All others features of the IDPrime .NET product family are immune, including all cryptographic features. Refer to the risk assessment below for a better understanding of the possible impacts.

Note that most Gemalto products implement Gemalto’s own cryptographic software libraries. These products are confirmed as not affected by this issue, and are therefore out of the scope of this advisory. Specifically, products in the IDPrime MD product family, which are proposed as the replacement product for the IDPrime .NET family, are immune to this vulnerability.
As security threats and attack vectors evolve daily, Gemalto continuously advises all customers to migrate from End-Of-Sale products to newer available products that provide the latest security features and are aligned with security regulations and standards world-wide. Gemalto has and is still proactively engaging customers to migrate from IDPrime.NET smart cards to the IDPrime MD smart card family.

Risk Assessment

Only RSA keys that are generated on-board by the IDPrime.NET product are potentially affected per the table below. Risk factors include:

1. The attacker needs to access the public key to proceed to the factorization and to get the private key.
2. The time and computing resources needed to compromise significantly depends on the key size (the longest, the stronger)
3. The compromise of one key pair does not tamper the security of the others keys, meaning that each product key has to be attacked independently.

The actual risk level strongly depends on each implementation use case. We therefore recommend that each organization using the IDPrime.NET products carry out their own risk assessment based on IDPrime.NET implementation and usage.

**Affected Products: IDPrime.NET family**

<table>
<thead>
<tr>
<th>Product versions</th>
<th>End of life announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDPrime.NET 510</td>
<td>July 31 2016</td>
</tr>
<tr>
<td>IDPrime.NET 511</td>
<td>July 31 2016</td>
</tr>
<tr>
<td>.NET Bio</td>
<td>July 31 2016</td>
</tr>
<tr>
<td>.NET Display Card</td>
<td>July 31 2016</td>
</tr>
<tr>
<td>IDPrime.NET 7519</td>
<td>Sept 4 2014</td>
</tr>
</tbody>
</table>

Mitigation Strategies

**Common Use Cases and recommendations**

There is no patch available due to the product’s tamper-resistant design. Migration to IDPrime MD product series, proposed as the replacement product for the IDPrime.NET, and not affected by that vulnerability, is recommended.

However, based on our analysis above, organizations can assess the following mitigations:

- **Data encryption use case:** usually the IDPrime.NET contains different key pairs for different usages. Encryption keys are generally generated on the server side (PKI Certificate Authority) for key escrow purposes. In such a case, encryption keys are not vulnerable and data encryption is not affected.

  *Recommendation:* Use only server generated keys. If encryption keys were generated on-board the IDPrime.NET card (a practice not recommended by the industry), customers should revoke and replace their current keys, with server-generated keys. It is also recommended to limit the distribution of any current public keys (that were generated on-board and IDPrime.NET) to trusted recipients only.
• **Data signing use case**: in this case, the public key is distributed to the recipients with the document (required for signature verification) which makes the public keys easily accessible.

  *Recommendation*: Where possible use server generated keys. Customers should revoke and replace their current keys, and store the newly server generated keys securely within the IDPrime.NET product which remains secure in this configuration.

• **Authentication use-case, including Microsoft smart-card logon**: usually the authentication key pair is dedicated for this use, with data signature (like S/MIME email signing or document/code signing) relying on a different key pair. In such a configuration, the public key is only shared between the user’s workstation and the target server. Key compromise in this use case would be complex and would require exploitation of others weaknesses in the IT infrastructure to succeed.

  *Recommendation*: Where possible use server generated keys. Customers should revoke and replace their current keys, and store the newly server generated keys securely within the IDPrime.NET product which remains secure in this configuration.

In addition, for critical applications, organizations can consider adding another layer of protection to the PKI-based authentication in the form of a login password or one-time password based solution.

• **Migration to IDPrime MD smart cards**

  Migrating to the IDPrime smart cards will resolve all use cases mentioned above without the need to generate server-side keys