# SSA-470231: TPM Vulnerability in SIMATIC IPCs

Publication Date: 2018-02-22
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 5.9

## SUMMARY

Several SIMATIC IPCs include a version of Infineon's Trusted Platform Module (TPM) firmware that mishandles RSA key generation. This makes it easier for attackers to conduct cryptographic attacks against the key material.

Siemens has released updates for the affected Industrial PCs.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC Field-PG M5:<br>BIOS < V22.01.04 | Update BIOS to V22.01.04<br>https://support.industry.siemens.com/cs/ww/en/view/109738122 |
| SIMATIC IPC227E:<br>BIOS < V20.01.10 | Update BIOS to V20.01.10<br>https://support.industry.siemens.com/cs/ww/en/view/109481715 |
| SIMATIC IPC277E:<br>BIOS < V20.01.10 | Update BIOS to V20.01.10<br>https://support.industry.siemens.com/cs/ww/en/view/109481715 |
| SIMATIC IPC427E (incl. SIPLUS variants):<br>BIOS < V21.01.07 | Update BIOS to V21.01.07<br>https://support.industry.siemens.com/cs/ww/en/view/109742593 |
| SIMATIC IPC477E:<br>BIOS < V21.01.07 | Update BIOS to V21.01.07<br>https://support.industry.siemens.com/cs/ww/en/view/109742593 |
| SIMATIC IPC547G:<br>BIOS < R1.21.0 | Update BIOS to R1.21.0<br>https://support.industry.siemens.com/cs/ww/en/view/109750349 |
| SIMATIC ITP1000:<br>BIOS < V23.01.03 | Update BIOS to V23.01.03<br>https://support.industry.siemens.com/cs/ww/en/view/109748173 |

## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Only RSA key pairs generated by the TPM are affected by this vulnerability. Rekeying of the TPM by using other cryptograhpic algorithms (e.g. ECC), using 3936-bit RSA keys, or importing RSA keys to the TPM that are generated by other systems help mitigate the security vulnerability.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

SIMATIC Industrial PCs are the PC hardware platform for PC-based Automation from Siemens.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

### Vulnerability CVE-2017-15361

The Infineon RSA library in Infineon Trusted Platform Module (TPM) firmware creates RSA keys which might be susceptible to the ROCA attack, possibly exposing the private key of a RSA key pair.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-310: Cryptographic Issues |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

## ADDITIONAL INFORMATION

Further information can be found on https://support.industry.siemens.com/cs/ww/de/view/109747626. Information about the vulnerability by Infineon can be found on https://www.infineon.com/cms/en/product/promopages/tpm-update/

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

V1.0 (2018-02-22): Publication Date
V1.1 (2018-03-15): Update for IPC547G
V1.2 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

## TERMS OF USE