

## SSA-470231: TPM Vulnerability in SIMATIC IPCs

Publication Date: 2018-02-22  
 Last Update: 2018-03-15  
 Current Version: V1.1  
 CVSS v3.0 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: BIOS < V22.01.04	Update BIOS to V22.01.04 <a href="https://support.industry.siemens.com/cs/ww/en/view/109738122">https://support.industry.siemens.com/cs/ww/en/view/109738122</a>
SIMATIC IPC227E: BIOS < V20.01.10	Update BIOS to V20.01.10 <a href="https://support.industry.siemens.com/cs/ww/en/view/109481715">https://support.industry.siemens.com/cs/ww/en/view/109481715</a>
SIMATIC IPC277E: BIOS < V20.01.10	Update BIOS to V20.01.10 <a href="https://support.industry.siemens.com/cs/ww/en/view/109481715">https://support.industry.siemens.com/cs/ww/en/view/109481715</a>
SIMATIC IPC427E: BIOS < V21.01.07	Update BIOS to V21.01.07 <a href="https://support.industry.siemens.com/cs/ww/en/view/109742593">https://support.industry.siemens.com/cs/ww/en/view/109742593</a>
SIMATIC IPC477E: BIOS < V21.01.07	Update BIOS to V21.01.07 <a href="https://support.industry.siemens.com/cs/ww/en/view/109742593">https://support.industry.siemens.com/cs/ww/en/view/109742593</a>
SIMATIC IPC547G: BIOS < R1.21.0	Update BIOS to R1.21.0 <a href="https://support.industry.siemens.com/cs/ww/en/view/109750349">https://support.industry.siemens.com/cs/ww/en/view/109750349</a>
SIMATIC ITP1000: BIOS < V23.01.03	Update BIOS to V23.01.03 <a href="https://support.industry.siemens.com/cs/ww/en/view/109748173">https://support.industry.siemens.com/cs/ww/en/view/109748173</a>

### 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 cryptographic 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 run the devices in a protected IT environment, Siemens particularly 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.

## **VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<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.

### 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 v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

## **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 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

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (<https://www.siemens.com/>

[terms\\_of\\_use](#), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.