PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

Cyber Security Advisory #02/2020

TPM-FAIL

Document Version: 1.1

First published: 2020-03-27
Last updated: 2020-06-18

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

B&R provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall B&R or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if B&R or its suppliers have been advised of the possibility of such damages.

Executive Summary

Cryptographic timing conditions in the subsystem for Intel(R) PTT before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.0 and 14.0.10; Intel(R) TXE 3.1.70 and 4.0.20; Intel(R) SPS before versions SPS_E5_04.01.04.305.0, SPS_SoC-X_04.00.04.108.0, SPS_SoC-A_04.00.04.191.0, SPS_E3_04.01.04.086.0, SPS_E3_04.08.04.047.0 may allow an unauthenticated user to potentially enable information disclosure via network access.
Selected B&R Products using Intel CPUs are vulnerable to Intel TPM-FAIL (CVE-2019-11090). The affected products are equipped with an independent hardware-based TPM. B&R recommends to use this one. Additionally B&R is in the process of creating BIOS updates.

Affected Products

Product	Affected Version	Notes
APC2200	BIOS version <1.13	
PPC2200	BIOS version <1.13	
APC3100	BIOS version <1.18	
PPC3100	BIOS version <1.18	
APC910	BIOS version <7.18	Only for B&R order number 5SWBIO.TS17-00

Vulnerability ID

CVE-2019-11090 TPM-FAIL in Intel firmware-based TPM

Vulnerability Severity

The severity assessment is based on the FIRST Common Vulnerability Scoring System (CVSS) v3.1.

CVE-2019-11090 TPM-FAIL in Intel firmware-based TPM

CVSS v3 Base Score: 6.8 (Medium)

CVSS v3 Vector: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N

Corrective Actions or Resolution

The described vulnerabilities will be fixed in the following product versions:

Product	Corrected Version	Availability date of patch
APC2200	BIOS version 1.13	2020-02-28
PPC2200	BIOS version 1.13	2020-02-28
APC3100	BIOS version 1.18	2020-02-28
PPC3100	BIOS version 1.18	2020-02-28
APC910	BIOS version 7.18	2020-06-18

B&R has already begun patching the affected BIOS versions. The release date will be published as soon as possible. Registered customers may approach their local B&R service organization in case of questions.

Vulnerability Details

CVE-2019-11090 TPM-FAIL in Intel firmware-based TPM

Description

A team of security researcher discovered a timing leakage flaw in Intel firmware-based TPM (fTPM). The vulnerability is named TPM-FAIL [1]. Intel published the cyber security advisory with CVE-2019-11090 [2]. The vulnerability relies on elliptic curve signature operations, such as ECDSA. The researchers were able to measure execution times of such operations inside the fTPM, to eventually extract the used private key.

Impact

The vulnerability may allow unauthenticated users to extract private keys, stored inside the fTPM.
A proof-of-concept code has been published by the security researchers [3].

Fix

B&R addresses the flaws by implementing the Intel patches for the affected BIOSs.

Workarounds and Mitigations

B&R has identified the following specific workarounds and mitigations.
The affected products come with a dedicated Infineon TPM chipset on the mainboard. Users of TPM should utilize this dedicated chip, rather than the Intel provided firmware-based TPM.

The affected B&R products do not come with initially stored secrets on the fTPM. Only customers explicitly utilizing the fTPM for elliptic curve signature operations are affected.

Supporting information and guidelines

The B&R Cyber Security webpage provides further information including Cyber Security guidelines.
Please find these resources here: https://www.br-automation.com/en/service/cyber-security/

References

[1] TPM-FAIL

`https://tpm.fail/`

[2] Intel Cyber Security Advisory on TPM-FAIL

`https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00241.html`

[3] Proof-of-concept exploit

`https://github.com/VernamLab/TPM-FAIL`

Document History

Version	Date	Description
1.0	2020-03-27	Initial version
1.1	2020-06-18	Update patch availabilities