SSA-501073: Vulnerabilities in Controllers CPU 1518 MFP using Intel CPUs (November 2020)

Publication Date: 2021-05-11
Last Update: 2022-03-08
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

Intel has published information on vulnerabilities in Intel products in November 2020. This advisory lists the Siemens Controllers that are affected by these vulnerabilities.

In this advisory we take a representative CVE from each advisory:

- “Intel CSME, SPS, TXE, AMT and DAL Advisory” Intel-SA-00391 is represented by CVE-2020-8744
- “BIOS Advisory” Intel-SA-00358 is represented by CVE-2020-0591.

Siemens is currently working on BIOS updates that include chipset microcode updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0, 6AG1518-4AX00-4AC0, incl. SIPLUS variant): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AC0): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Avoid to run untrusted code on affected systems

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

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the STEP 7 program if required.

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-2020-0591

Improper buffer restrictions in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-8744

Improper initialization in subsystem for Intel(R) CSME versions before 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel(R) TXE versions before 4.0.30 Intel(R) SPS versions before E3_05.01.04.200 may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-665: Improper Initialization

ADDITIONAL INFORMATION

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 (2021-05-11): Publication Date
V1.1 (2022-03-08): Updated specific mitigations; clarified that no remediation is planned

TERMS OF USE