SSA-686975: IPU 2022.3 Vulnerabilities in Siemens Industrial Products using Intel CPUs

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.9

SUMMARY

Intel has published information on vulnerabilities in Intel products in November 2022. This advisory lists the related Siemens Industrial products affected by these vulnerabilities that can be patched by applying the corresponding BIOS update ("2022.3 IPU – BIOS Advisory" Intel-SA-00688).

Siemens is preparing 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 Field PG M5: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC427E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC BX-39A: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIMATIC ITP1000: All versions	Currently no fix is available 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:

- As a prerequisite for an attack, an attacker must be able to run untrusted code on affected systems. Siemens recommends limiting the possibilities to run untrusted code if possible.

Please follow the General Security Recommendations.

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 Field PG is a mobile, industry-standard programming device for automation engineers with all commonly used interfaces for industrial applications that also brings pre-installed SIMATIC engineering software.

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based automation from Siemens.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (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-2022-21198

Time-of-check time-of-use race condition in the 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	7.9
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

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 (2023-02-14): Publication Date

TERMS OF USE