

SSA-981975: Information Disclosure Vulnerability in Intel-CPUs (CVE-2022-40982) Impacting SIMATIC IPCs

Publication Date: 2023-09-12
Last Update: 2023-11-14
Current Version: V1.1
CVSS v3.1 Base Score: 6.5

SUMMARY

Several Intel-CPU based SIMATIC IPCs are affected by an information exposure vulnerability (CVE-2022-40982) in the CPU that could allow an authenticated local user to potentially read other users' data [1].

The issue is also known as "Gather Data Sampling" (GDS) or Downfall Attacks. For details refer to the chapter "Additional Information".

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

[1] <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html>

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Field PG M6: 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 IPC1047: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC1047E: 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 IPC PX-39A: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC PX-39A PRO: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC RW-543A: 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:

- Ensure that only trusted persons have access to the system and avoid the configuration of additional accounts

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-2022-40982

Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

ADDITIONAL INFORMATION

- INTEL Security Advisory: <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html>
- Gather Data Sampling (GDS), details: <https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/gather-data-sampling.html>
- Downfall Attacks: <https://downfall.page/>

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 (2023-09-12):	Publication Date
V1.1 (2023-11-14):	Added SIMATIC IPC 1047/1047E

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.