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

Publication Date: 2023-09-12
Last Update: 2024-07-09
Current Version: V1.2
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 has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes 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 affected by CVE-2022-40982	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E / IPC647E / IPC677E / IPC847E:	Update to V25.02.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All versions < V25.02.14 affected by CVE-2022-40982	Update to V25.02.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All versions < V25.02.14 affected by CVE-2022-40982	Update to V25.02.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All versions < V25.02.14 affected by CVE-2022-40982	Update to V25.02.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations

SIMATIC IPC847E: All versions < V25.02.14 affected by CVE-2022-40982	Update to V25.02.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC1047: All versions affected by CVE-2022-40982	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC1047E: All versions affected by CVE-2022-40982	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC BX-39A / IPC PX-39A / IPC PX-39A PRO:	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC BX-39A: All versions affected by CVE-2022-40982	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC PX-39A: All versions affected by CVE-2022-40982	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC PX-39A PRO: All versions affected by CVE-2022-40982	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC IPC RW-543A: All versions < V1.1.2 affected by CVE-2022-40982	Update to V1.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408/ See further 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

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. 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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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
V1.2 (2024-07-09):	Added fix for SIMATIC IPC627E / IPC647E / IPC677E / IPC847E and for SIMATIC IPC RW-543A

TERMS OF USE