SSA-784849: Direct Memory Access Vulnerabilities in SIMATIC CP Devices

Publication Date: 2023-10-10
Last Update: 2023-10-10
Current Version: V1.0
CVSS v3.1 Base Score: 6.7

SUMMARY

Several SIMATIC CP devices contain direct memory access vulnerabilities that could allow an attacker to execute code, access the PROFINET network without restrictions or perform denial of service attacks.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1604 (6GK1160-4AA01): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1616 (6GK1161-6AA02): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1623 (6GK1162-3AA00): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1626 (6GK1162-6AA01): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1628 (6GK1162-8AA00): All versions	Currently no fix 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:

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

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 CP 1623, CP 1626 and CP 1628 are PCI express cards for connection to Industrial Ethernet.

SIMATIC CP 1604 and CP 1616 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

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-2023-37194

The kernel memory of affected devices is exposed to user-mode via direct memory access (DMA) which could allow a local attacker with administrative privileges to execute arbitrary code on the host system without any restrictions.

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:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2023-37195

Affected devices insufficiently control continuous mapping of direct memory access (DMA) requests. This could allow local attackers with administrative privileges to cause a denial of service situation on the host. A physical power cycle is required to get the system working again.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Thomas Riedmaier from Siemens Energy for reporting the vulnerabilities

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 (2023-10-10): Publication Date

TERMS OF USE