SSA-620338: Buffer Overflow Vulnerability in SICAM AK3 / BC / TM

Publication Date: 2024-06-11
Last Update: 2024-06-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 7.3

SUMMARY

SICAM AK3/TM/BC devices are affected by a buffer overflow vulnerability that could allow an attacker to execute code in the context of the current process or lead to a denial of service condition.

- SICAM AK3 device firmware
  - CPCX26 for CP-2016
  - PCCX26 for CP-2019
- SICAM AK3, SICAM BC and SICAM TM device firmware
  - ETA4 and ETA5 for SM-2558

Siemens has released new firmware versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
CPCX26 Central Processing/Communication: All versions < V06.02 affected by CVE-2024-31484	Update to V06.02 or later version. The firmware CPCX26 V06.02 is present within “SICAM RTUs AK3 Package” V06.02 https://support.industry.siemens.com/cs/ww/en/view/109813252/
ETA4 Ethernet Interface IEC60870-5-104: All versions < V10.46 affected by CVE-2024-31484	Update to V10.46 or later version The firmware ETA4 V10.46 is present within “SICAM RTUs AK3 Package” V06.02 https://support.industry.siemens.com/cs/ww/en/view/109813252/
ETA5 Ethernet Int. 1x100TX IEC61850 Ed.2: All versions < V03.27 affected by CVE-2024-31484	Update to V03.27 or later version The firmware ETA5 V03.27 is present within “SICAM RTUs AK3 Package” V06.02 https://support.industry.siemens.com/cs/ww/en/view/109813252/
PCCX26 Ax 1703 PE, Contr, Communication Element: All versions < V06.05 affected by CVE-2024-31484	Update to V06.05 or later version The firmware PCCX26 V06.05 is present within “SICAM RTUs AK3 Package” V06.02 https://support.industry.siemens.com/cs/ww/en/view/109813252/

WORKAROUNDS AND MITIGATIONS

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

SICAM AK 3 is a telecontrol and automation device facilitating the automation of diverse processes across widely distributed systems.

SICAM BC is a bay control device with a standardized communication interface.

SICAM TM is an automation and telecontrol system with a standardized communication interface.

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-2024-31484

The affected devices contain an improper null termination vulnerability while parsing a specific HTTP header. This could allow an attacker to execute code in the context of the current process or lead to denial of service condition.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	7.3
CVSS Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-170: Improper Null Termination

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Steffen Robertz from SEC Consult Vulnerability Lab for coordinated disclosure of the vulnerability

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 (2024-06-11): Publication Date

TERMS OF USE