SSA-658793: Command Injection Vulnerability in SiPass integrated AC5102 / ACC-G2 and ACC-AP

Publication Date: 2023-02-14
Last Update: 2023-02-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

SiPass integrated ACC (Advanced Central Controller) devices improperly sanitize user input on the telnet command line interface. This could allow an authenticated user to escalate privileges by injecting arbitrary commands that are executed with root privileges.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SiPass integrated AC5102 (ACC-G2): All versions < V2.85.44	Update to V2.85.44 or later version https://support.industry.siemens.com/cs/ww/en/view/109814044/ See further recommendations from section Workarounds and Mitigations
SiPass integrated ACC-AP: All versions < V2.85.43	Update to V2.85.43 or later version https://support.industry.siemens.com/cs/ww/en/view/109814044/ 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:

- Set individual passwords for the main accounts provided in the ACC firmware (SIEMENS, OPERATOR)
- Disable telnet access

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 affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

ACC-AP (Advanced Central Controller) is a door controller for up to two doors connected to an Internet/Intranet network for communication with the SiPass integrated access control system.

AC5102 / ACC-G2 (Advanced Central Controller) is the central controller for SiPass integrated access control systems.

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-2022-31808

Affected devices improperly sanitize user input on the telnet command line interface.

This could allow an authenticated user to escalate privileges by injecting arbitrary commands that are executed with root privileges.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Airbus Security for reporting the vulnerability

ADDITIONAL INFORMATION

The fix for CVE-2022-31808 is part of the ACC platform firmware version V4.1.10. The firmware V2.85.43 (released for ACC-AP) includes platform version V4.1.10. The firmware V2.85.44 (released for ACC-G2) includes platform version V4.1.12.

The new versions are released for both SiPass integrated version lines:

- V2.85, see https://support.industry.siemens.com/ww/en/view/109801507/
- V2.90, see https://support.industry.siemens.com/ww/en/view/109814044/

Note that CVE-202-31808 also affects the following products, which are out of support already. Therefore, no fix release is planned for:

- SiPass integrated AC5100 (ACC)
- SiPass integrated AC5200 (ACC-Lite, ACC-4, ACC-8, ACC-16, ACC-32)

- SiPass integrated Granta-MK3 (ACC-GRANTA)

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