SSA-924149: Stack Overflow Vulnerability in SiPass Integrated before V2.90.3.8

Publication Date: 2023-07-11
Last Update: 2023-07-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SiPass integrated versions before V2.90.3.8 contain a stack overflow vulnerability that could allow an unauthenticated remote attacker to crash the server application, creating a denial of service condition.

Siemens has released an update for SiPass integrated and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SiPass integrated: All versions < V2.90.3.8	Update to V2.90.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109814044/

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 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

SiPass integrated is a powerful and extremely flexible access control system.

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-2022-31810

Affected server applications improperly check the size of data packets received for the configuration client login, causing a stack-based buffer overflow.

This could allow an unauthenticated remote attacker to crash the server application, creating a denial of service condition.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/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

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 (2023-07-11): Publication Date

TERMS OF USE