SSA-978558: Insufficient Logging Vulnerability in SIPORT MP

Publication Date: 2020-02-11
Last Update: 2020-02-11
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

SIPORT MP version 3.1.4 fixes a vulnerability that allowed to create special accounts (“service users”) which could enable an authenticated attacker to perform actions that are invisible to other users of the system.

Siemens recommends customers to apply the update. For older versions, a hotfix and a tool are available to mitigate the vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPORT MP: All versions < 3.1.4	Update to version 3.1.4 https://support.industry.siemens.com/cs/document/109771860 (login required)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- For SIPORT MP versions 3.0.x, apply the latest hotfix for version 3.0.3, available at https://support.industry.siemens.com/cs/document/109771281
- For SIPORT MP versions 2.2 and later, apply the SIPORT_CleanUsers tool, available at https://support.industry.siemens.com/cs/document/109771860

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

SIPORT is a comprehensive, modular and reliable system for access control and time management within the SSP Siveillance Access Suite.

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-2019-19277

Vulnerable versions of the device allow the creation of special accounts (“service users”) with administrative privileges that could enable a remote authenticated attacker to perform actions that are not visible to other users of the system, such as granting persons access to a secured area.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-778: Insufficient Logging

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 (2020-02-11): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.