SSA-384879: Authentication Bypass Vulnerability in SIPORT MP

Publication Date:	2020-10-13
Last Update:	2020-10-13
Current Version:	V1.0
CVSS v3.1 Base Score:	8.8

SUMMARY

SIPORT MP version 3.2.1 fixes an authentication bypass vulnerability which could enable an attacker to impersonate other users of the system and perform administrative actions.

Siemens recommends to apply the update.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPORT MP: All versions < 3.2.1	Update to version 3.2.1 https://support.industry.siemens.com/cs/ww/en/view/109781856 (login required)

WORKAROUNDS AND MITIGATIONS

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

- For installations where the update to version 3.2.1 is not possible: contact your local Siemens support for deployment-specific mitigation measures

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 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-2020-7591

Vulnerable versions of the device could allow an authenticated attacker to impersonate other users of the system and perform (potentially administrative) actions on behalf of those users if the single sign-on feature (“Allow logon without password”) is enabled.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CWE	CWE-603: Use of Client-Side Authentication

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 (2020-10-13):	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.