SSA-160202: Multiple Access Control Vulnerabilities in SiPass Integrated

Publication Date: 2021-12-14
Last Update: 2021-12-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SiPass integrated contains multiple vulnerabilities that could allow an unauthenticated remote attacker to access or modify several internal application resources.

Siemens has released a tool, “SiPass integrated Component Manager”, to remediate the vulnerabilities on all maintained and supported versions of SiPass integrated and recommends to apply this tool.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SiPass integrated V2.76: All versions	Update to V2.76 SP2 and then download and execute the SiPass integrated Component Manager: https://support.industry.siemens.com/cs/ww/en/view/109802587/
SiPass integrated V2.80: All versions	Download and execute the SiPass integrated Component Manager: https://support.industry.siemens.com/cs/ww/en/view/109802587/
SiPass integrated V2.85: All versions	Download and execute the SiPass integrated Component Manager: https://support.industry.siemens.com/cs/ww/en/view/109802587/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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-2021-44522

Affected applications insufficiently limit the access to the internal message broker system.

This could allow an unauthenticated remote attacker to subscribe to arbitrary message queues.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2021-44523

Affected applications insufficiently limit the access to the internal activity feed database.

This could allow an unauthenticated remote attacker to read, modify or delete activity feed entries.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2021-44524

Affected applications insufficiently limit the access to the internal user authentication service.

This could allow an unauthenticated remote attacker to trigger several actions on behalf of valid user accounts.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

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 (2021-12-14): 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.