SSA-339433: Vulnerabilities in SiPass integrated

Publication Date 2017-07-12
Last Update 2017-07-12
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

The latest release V2.70 of SiPass integrated resolves multiple vulnerabilities. One of these vulnerabilities could allow an unauthenticated attacker with network access to the server to perform administrative operations.

Siemens recommends updating to the new version.

AFFECTED PRODUCTS

- SiPass integrated: All versions < V2.70

DESCRIPTION

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

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-9939)

An attacker with network access to the SiPass integrated server could bypass the authentication mechanism and perform administrative operations.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2017-9940)

An attacker with access to a low-privileged user account can read or write files on the file system of the SiPass integrated server over the network.

CVSS Base Score 8.1
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability 3 (CVE-2017-9941)

An attacker in a Man-in-the-Middle position between the SiPass integrated server and SiPass integrated clients could read or modify the network communication.

CVSS Base Score 7.4
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability 4 (CVE-2017-9942)

An attacker with local access to the SiPass integrated server or SiPass integrated client could potentially obtain credentials from the systems.

CVSS Base Score 6.2
CVSS Vector CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

SOLUTION

Siemens provides SiPass integrated V2.70 [1], which fixes the vulnerabilities, and recommends customers to update to the new version.

ADDITIONAL RESOURCES

[1] The new version of SiPass integrated can be obtained from Siemens customer support or from authorized value-added partners.

[2] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-07-12): Publication Date

DISCLAIMER