

SSA-946325: Vulnerabilities in SICAM PAS

Publication Date 2016-11-25
Last Update 2016-11-25
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

SICAM PAS products are affected by multiple vulnerabilities which could cause a Denial of Service condition and could potentially lead to remote code execution.

SICAM PAS versions 8.00 and higher fix two of the vulnerabilities. For the two remaining vulnerabilities, Siemens recommends detailed mitigations and is preparing software updates.

AFFECTED PRODUCTS

- SICAM PAS: All versions

DESCRIPTION

SICAM PAS is an energy automation solution for operating an electrical substation with its devices.

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-2016-8567)

A factory account with hardcoded passwords is present in the SICAM PAS installations. Attackers might gain privileged access to the database over port 2638/TCP.

SICAM PAS versions 8.00 and higher are not affected by this vulnerability.

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-2016-8566)

An authenticated local attacker with certain privileges could possibly reconstruct passwords of users for accessing the database.

SICAM PAS versions 8.00 and higher are not affected by this vulnerability.

CVSS Base Score 7.8

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

Vulnerability 3 (CVE-2016-9156)

A remote attacker could use specially crafted packets sent to port 19235/TCP to upload, download or delete files in certain parts of the file system.

CVSS Base Score 7.3

CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:T/RC:C

Vulnerability 4 (CVE-2016-9157)

Specially crafted packets sent to port 19234/TCP could cause a Denial of Service condition and potentially lead to unauthenticated remote code execution.

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:T/RC:C

Mitigating Factors

The attacker must have network access to the SICAM PAS system for vulnerabilities 1, 3, 4 and local access for vulnerability 2.

SOLUTION

SICAM PAS versions 8.00 and higher fix vulnerabilities 1 and 2. Siemens recommends customers upgrade to the latest version.

For vulnerability 3 and 4 Siemens recommends customers explicitly block access to ports 19235/TCP and 19234/TCP with appropriate mechanism, e.g. using the Windows firewall, until patches are available.

As a general security measure, Siemens recommends to protect network access with appropriate mechanisms [2] (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Ilya Karpov, Positive Technologies for coordinated disclosure of vulnerability 1.
- Ilya Karpov and Dmitry Sklyarov, Positive Technologies for coordinated disclosure of vulnerability 2.
- Sergey Temnikov and Vladimir Dashchenko, Critical Infrastructure Defense Team, Kaspersky Lab for coordinated disclosure of vulnerabilities 3 and 4.

ADDITIONAL RESOURCES

[1] In order to receive the SICAM PAS V8.08 update, please contact your regional Siemens representative or Siemens Energy Customer Support Center at:

support.energy@siemens.com

[2] Information about Industrial Security by Siemens:

<https://www.siemens.com/gridsecurity>

[3] 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 (2016-11-25): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use