SSA-444217: Information Disclosure Vulnerabilities in SICAM PAS

Publication Date 2016-06-30
Last Update 2016-11-25
Current Version V1.1
CVSSv3 Base Score 2.5

SUMMARY

Siemens has released SICAM PAS version 8.08 which fixes two information disclosure vulnerabilities that could allow authenticated local operating system users to obtain sensitive information under certain conditions.

AFFECTED PRODUCTS

- SICAM PAS: All versions < 8.08

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 (CVSSv3.0) (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 defined by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2016-5848)

An authenticated local attacker with certain privileges to the SICAM PAS database could possibly reconstruct passwords for SICAM PAS users.

CVSS Base Score 2.3
CVSS Vector CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2016-5849)

An authenticated local attacker could possibly access sensitive configuration information from the SICAM PAS database file if the database is in a stopped state.

CVSS Base Score 2.5
CVSS Vector CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have local access to the SICAM PAS system and certain database privileges or the database must be in a stopped state.

SOLUTION

Siemens provides SICAM PAS 8.08 which fixes the vulnerabilities and recommends customers to update to this version [1].

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 from Positive Technologies for coordinated disclosure of vulnerability 1.
- Ilya Karpov and Dmitry Sklyarov from Positive Technologies for coordinated disclosure of vulnerability 2.

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] Recommended security guidelines to Secure Substation: https://www.siemens.com/gridsecurity (Select “Cyber Security General Downloads” tab → “Manuals”)

[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 (2016-06-30): Publication Date

V1.1 (2016-11-25): Added fix information for vulnerability 2

DISCLAIMER