SSA-579309: Denial-of-Service in SICAM A8000 Series

Publication Date: 2019-01-08
Last Update: 2019-02-12
Current Version: V1.1
CVSS v3.0 Base Score: 5.3

SUMMARY

The SICAM A8000 RTU series is affected by a security vulnerability that could allow unauthenticated remote users to cause a Denial-of-Service (DoS) condition of the web server of affected products.

Siemens has released updates for all product variants and recommends that customers update to the new versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICAM A8000 CP-8000: All versions < V14	Update to V14 https://support.industry.siemens.com/cs/search?search=a8000%20cp8000
SICAM A8000 CP-802X: All versions < V14	Update to V14 https://support.industry.siemens.com/cs/search?search=a8000%20cp8000
SICAM A8000 CP-8050: All versions < V2.00	Update to V2.00 or higher https://support.industry.siemens.com/cs/search?search=a8000%20cp8050

WORKAROUNDS AND MITIGATIONS

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

- Limit access to the web server on port 80/TCP and 443/TCP with an external firewall.
- Apply a Defence-in-Depth strategy.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (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.

Recommended security guidelines to Secure Substations can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

The SICAM A8000 RTU (Remote Terminal Unit) series is a modular device range for telecontrol and automation applications in all areas of energy supply.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-13798

Specially crafted network packets sent to port 80/TCP or 443/TCP could allow an unauthenticated remote attacker to cause a Denial-of-Service condition of the web server.

The security vulnerability could be exploited by an attacker with network access to the affected systems on port 80/TCP or 443/TCP. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the web server. A system reboot is required to recover the web service of the device.

At the time of advisory update, exploit code for this security vulnerability is public.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:H/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Emanuel Duss and Nicolas Heiniger from Compass Security for coordinated disclosure

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 (2019-01-08):	Publication Date
V1.1 (2019-02-12):	Adapted CVSS vector due to known exploit

TERMS OF USE