# SSA-751155: Denial-of-Service Vulnerability in SCALANCE S613

Publication Date 2016-04-08
Last Update 2016-04-08
Current Version V1.0
CVSSv3 Base Score 5.3

## SUMMARY

A vulnerability in SCALANCE S613 could allow unauthenticated remote attackers to cause a Denial-of-Service of the web server under certain conditions.

Siemens recommends that customers contact Siemens customer support [1] in order to obtain advice on a solution for the customer's specific environment.

## AFFECTED PRODUCTS

- SCALANCE S613 (MLFB: 6GK5613-0BA00-2AA3): All versions

## DESCRIPTION

The SCALANCE S firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways. SCALANCE S613 are designed for extended temperature environments and provide additional security functionality, e.g. VPN tunnels.

Detailed information about the vulnerability is provided below.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSSv3) (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 (CVE-2016-3963)

Certain legitimate messages sent to port 443/tcp could cause a Denial-of-Service of the integrated web server of affected devices. A manual reboot is required to recover the web server of the device.

CVSS 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:P/RL:W/RC:C

Mitigating Factors

In order to exploit the vulnerability, the attacker must have network access to the port 443/tcp on the affected devices.

## SOLUTION

Siemens recommends that customers contact Siemens customer support [1] in order to obtain advice on a solution for the customer's specific environment.

## ADDITIONAL RESOURCES

[1] Siemens support can be contacted via mail at support.automation@siemens.com or via phone +49 (911) 895-7222

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] 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 (2016-04-08): Publication Date

## DISCLAIMER