SSA-342135: Web Vulnerability in SCALANCE M-800 / S615

Publication Date 2016-09-22
Last Update 2016-09-22
Current Version V1.0
CVSS v3.0 Base Score 4.0

SUMMARY

Siemens has released an update for SCALANCE M-800 / S615 modules which fixes a security vulnerability that could allow an attacker in a privileged network position to obtain web session cookies under certain circumstances.

AFFECTED PRODUCTS

SCALANCE M-800 / S615: All versions < V4.02

DESCRIPTION

The SCALANCE M industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

The SCALANCE S firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections and provides 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 3.0 (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 Description (CVE-2016-7090)

The integrated web server delivers session cookies without the “secure” flag. Modern browsers interpreting the flag would mitigate potential data leakage in case of clear text transmission.

CVSS Base Score 4.0
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

SOLUTION

Siemens provides firmware version V4.02 [1] for SCALANCE M-800 / S615 modules that fixes the vulnerability and recommends customers to update to the new version.

As a general security measure Siemens strongly recommends to protect network access to the management interface to SCALANCE M-800 / S615 modules with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2].

ACKNOWLEDGEMENTS

Siemens thanks Alexander Van Maele and Tijl Deneut from HOWEST for coordinated disclosure.

ADDITIONAL RESOURCES

[1] Firmware version V4.02 for Scalance M-800 / S615 can be obtained for free from: https://support.industry.siemens.com/cs/ww/en/view/109740858

[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 (2016-09-22): Publication Date

DISCLAIMER