SSA-977428: Vulnerabilities in SCALANCE M875

Publication Date: 2018-06-12
Last Update: 2018-06-12
Current Version: V1.0
CVSS v3.0 Base Score: 7.5

SUMMARY

Multiple vulnerabilities have been identified in the web interface of SCALANCE M875. The web interface of SCALANCE M875 could allow Cross-Site Request Forgery (CSRF), stored Cross-Site Scripting (XSS), or command injection attacks if an attacker is authenticated or tricks a legitimate authenticated user into accessing a malicious link.

Siemens recommends customers to upgrade their hardware, and provides mitigations until hardware upgrades can be applied.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE M875: All versions	Upgrade hardware to SCALANCE M876-4 or RUGGEDCOM RM1224, or follow recommendations from Section Workarounds and Mitigations.

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the web-based management interface to the internal or VPN network.
- Use the built-in firewall to further restrict access to the web interface to trusted IP addresses if possible.
- Protect administrative user account with strong passwords.
- Do not browse other websites and do not click on external links while being authenticated to the administrative web interface.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT 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.

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-2018-4859

An authenticated remote attacker with access to the web interface (443/tcp), could execute arbitrary operating system commands.

Successful exploitation requires that the attacker has network access to the web interface. The attacker must be authenticated as administrative user to exploit the security vulnerability.

The vulnerability could allow an attacker to execute arbitrary code on the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.2
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-4860

An authenticated remote attacker with access to the web interface (443/tcp), could execute arbitrary operating system commands.

Successful exploitation requires that the attacker has network access to the web interface. The attacker must be authenticated as administrative user to exploit the security vulnerability.

The vulnerability could allow an attacker to execute arbitrary code on the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.2
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-4861

An authenticated remote attacker with access to the web interface (443/tcp), could potentially read and download arbitrary files from the device's file system.

Successful exploitation requires that the attacker has network access to the web interface. The attacker must be authenticated as administrative user to exploit the security vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	4.9
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-11447

The web interface on port 443/tcp could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

Successful exploitation requires user interaction by an legitimate user, who must be authenticated to the web interface as administrative user. A successful attack could allow an attacker to interact with the web interface as an administrative user. This could allow the attacker to read or modify the device configuration, or to exploit other vulnerabilities that require authentication as administrative user.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11448

The web interface on port 443/tcp could allow a stored Cross-Site Scripting (XSS) attack if an unsuspecting user is tricked into accessing a malicious link.

Successful exploitation requires that the attacker has access to the web interface of an affected device. The attacker must be authenticated as administrative user on the web interface. Afterwards, a legitimate user must access the web interface.

A successful attack could allow an attacker to execute malicious code in the browser of a legitimate user.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	4.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-11449

An attacker with access to the local file system might obtain passwords for administratrive users.

Successful exploitation requires read access to files on the local file system. A successful attack could allow an attacker to obtain administrative passwords.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	4.4
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Eugenie Potseluevskaya from Kaspersky Lab 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 (2018-06-12): Publication Date

TERMS OF USE