SSA-689071: DNSMasq Vulnerabilities in SCALANCE W1750D, SCALANCE M-800 / S615 and RUGGEDCOM RM1224

Publication Date: 2017-11-17
Last Update: 2020-10-13
Current Version: V1.3
CVSS v3.1 Base Score: 8.1

SUMMARY

Multiple vulnerabilities have been identified in SCALANCE W1750D, SCALANCE M-800 / S615 and RUGGEDCOM RM1224 devices. The highest scored vulnerability could allow a remote attacker to crash the DNS service or execute arbitrary code. The attacker must be able to craft malicious DNS responses and inject them into the network in order to exploit the vulnerability.

Siemens has released updates for the affected devices, recommends to update, and provides specific countermeasures for unpatched devices.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: All versions < V5.0	Update to V5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109757544
SCALANCE M-800 / S615: All versions < V5.0	Update to V5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109757544
SCALANCE W1750D: All versions < V6.5.1.5	Update to V6.5.1.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109778052

WORKAROUNDS AND MITIGATIONS

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

- SCALANCE M-800 / S615 and RUGGEDCOM RM1224: Disable DNS proxy in the device configuration (System - DNS - DNS Proxy - Disable Checkbox „Enable DNS Proxy“), and configure the connected devices in the internal network to use a different DNS server
- SCALANCE W1750D: If “OpenDNS”, “Captive Portal” or “URL redirection” functionality is not used, deploy firewall rules in the device configuration to block incoming access to port 53/UDP

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 W1750D controller-based Direct Access Points support radio transmission according to the latest IWLAN standard IEEE 802.11ac Wave 2.

The SCALANCE M-800 / S615 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.

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio, optimized for use in North America.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2017-13704

An attacker could cause a crash of the DNSmasq process by sending specially crafted request messages to the service on port 53/udp.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2017-14491

An attacker could cause a crash or potentially execute arbitrary code by sending specially crafted DNS responses to the DNSmasq process. In order to exploit this vulnerability, an attacker must be able to trigger DNS requests from the device, and must be in a privileged position to inject malicious DNS responses.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2017-14495

An attacker could cause a crash of the DNSmasq process by sending specially crafted request messages to the service on port 53/udp.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2017-14496

An attacker could cause a crash of the DNSmasq process by sending specially crafted request messages to the service on port 53/udp.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

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 (2017-11-17):	Publication Date
V1.1 (2018-04-05):	Changed to the new format and added update information for SCALANCE W1750D
V1.2 (2018-05-09):	Added update information for SCALANCE M-800 / S615
V1.3 (2020-10-13):	Added RUGGEDCOM RM1224 and updated remediation link for SCALANCE W1750D; updated CVSS scores and added CWE IDs; additional editorial changes

TERMS OF USE