

SSA-646763: DNSpooq - Dnsmasq Vulnerabilities in SCALANCE and RUGGEDCOM Devices

Publication Date: 2021-01-19
 Last Update: 2021-03-09
 Current Version: V1.1
 CVSS v3.1 Base Score: 4.0

SUMMARY

Security researchers discovered and disclosed seven vulnerabilities in the open-source DNS component “dnsmasq”, also known as “DNSpooq” vulnerabilities (CVE-2020-25681 through CVE-2020-25687). Three vulnerabilities (CVE-2020-25684 through CVE-2020-25686) affect the validation of DNS responses and impact several SCALANCE and RUGGEDCOM devices as listed below.

Siemens is preparing updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE M-800: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE S615: All versions	See recommendations from section Workarounds and Mitigations
SCALANCE SC-600: All versions < V2.1.3	Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109793041/
SCALANCE W1750D: All versions	See 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:

- SCALANCE M-800: 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. Note that the DNS proxy is enabled by default.
- RUGGEDCOM RM1224: Same as for SCALANCE M-800. Note that the DNS proxy is enabled by default.
- SCALANCE S615: Same as for SCALANCE M-800. Note that the DNS proxy is disabled by default.
- SCALANCE SC-600: Same as for SCALANCE M-800. Note that the DNS proxy is disabled by default.
- 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

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio.

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.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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

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-2020-25684

Affected devices lack proper address/port check in the DNS reply_query function of dnsmasq.

This could make it easier for remote off-path attackers to forge replies.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability CVE-2020-25685

Affected devices lack query resource name (RRNAME) checks in the DNS reply_query function of dnsmasq.

This could allow a remote attacker to spoof DNS traffic that can lead to DNS cache poisoning.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability CVE-2020-25686

Affected devices lack sufficient entropy in dnsmasq to handle multiple DNS query requests from the same resource name (RRNAME).

This could allow a remote attacker to spoof DNS traffic, using a birthday attack (RFC 5452), than can lead to DNS cache poisoning.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Moshe Kol and Shlomi Oberman from JSOF for coordinated disclosure
- CERT Coordination Center (CERT/CC) for coordination efforts
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

ADDITIONAL INFORMATION

For more details regarding the DNSpooq vulnerabilities in dnsmasq refer to:

- [JSOF Publication "DNSpooq"](#)
- [CERT/CC Advisory VU#434904](#)

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 (2021-01-19): Publication Date
V1.1 (2021-03-09): Added solution for SCALANCE SC-600

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.