SSA-689071: DNSMasq Vulnerabilities in SCALANCE W1750D, SCALANCE M800 and SCALANCE S615

Publication Date: 2017-11-17
Last Update: 2018-04-05
Current Version: V1.1
CVSS v3.0 Base Score: 8.1

SUMMARY

Multiple vulnerabilities have been identified in SCALANCE W1750D, SCALANCE M800, and SCALANCE S615 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 is working on updates for the affected devices, and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE M800 / S615: All versions	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: All versions < V6.5.1.5-4.3.1.8	Install V6.5.1.5-4.3.1.8. Customers who do not use the “OpenDNS”, “Captive Portal” or “URL redirection” functionality, can alternatively deploy firewall rules in the device configuration to block incoming access to port 53/UDP. https://support.industry.siemens.com/cs/ww/en/view/109756771

WORKAROUNDS AND MITIGATIONS

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

- Apply Defense-in-Depth

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly 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

 © Siemens AG 2018

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 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 in different ways.

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-2017-13704

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

CVSS v3.0 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:T/RC:C

Vulnerability CVE-2017-14491

An attacker can cause a crash or potentially execute arbitrary code by sending speciallycrafted DNS responses to the DNSmasq process. In order to exploit this vulnerability, anattacker must be able to trigger DNS requests from the device, and must be in a positionthat allows him to inject malicious DNS responses, e.g. the attacker must be in a Man-inthe-Middleposition.

CVSS v3.0 Base Score	8.1
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2017-14495

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

CVSS v3.0 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:T/RC:C

Vulnerability CVE-2017-14496

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

CVSS v3.0 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:T/RC:C

ADDITIONAL INFORMATION

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 (2017-11-17): Publication Date
V1.1 (2018-04-05): Changed to the new format and added update information for SCALANCE W1750D

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.