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

Publication Date 2017-11-17
Last Update 2017-11-17
Current Version V1.0
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

- SCALANCE W1750D: All versions
- SCALANCE M800 / S615: All versions

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 and provides additional security functionality, e.g. VPN tunnels.

Detailed information about the vulnerabilities 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 1 (CVE-2017-13704)

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

CVSS 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 2 (CVE-2017-14491)

An attacker can 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 position that allows him to inject malicious DNS responses, e.g. the attacker must be in a Man-in-the-Middle position.

CVSS 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 3 (CVE-2017-14495)

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

CVSS 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 4 (CVE-2017-14496)

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

CVSS 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

Mitigating Factors

SCALANCE W1750D devices that are operated in controller mode on an Aruba Mobility Controller are not affected if AOS versions newer than V6.3.1.25, V6.4.4.16 V6.5.1.9, V6.5.3.3, V6.5.4.2, or 8.1.0.4 are used.

An attacker must be in the internal network in order to exploit vulnerabilities 1, 3, and 4.

SOLUTION

Siemens is preparing updates for the affected products and recommends the following mitigations until patches are available:

- For SCALANCE W1750D: Customers who do not use the “OpenDNS”, “Captive Portal” or “URL redirection” functionality, can deploy firewall rules in the device configuration to block incoming access to port 53/UDP.
- For SCALANCE M800/S615: 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.
- Apply Defense-in-Depth [1]

It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[2] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[3] 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

DISCLAIMER