SSA-324955: SAD DNS Attack in Linux Based Products

Publication Date: 2021-05-11
Last Update: 2021-07-13
Current Version: V1.2
CVSS v3.1 Base Score: 7.4

SUMMARY

A vulnerability made public under the name SAD DNS affects Domain Name System resolvers due to a vulnerability in the Linux kernel when handling ICMP packets. The Siemens products which are affected are listed below. For more information please see https://www.saddns.net/.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224: All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE M-800: All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
SCALANCE S615: All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/
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: V8.3.0.1, V8.6.0 and V8.7.0	See recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC MV500 family: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1243-1 (incl. SIPLUS variants): All versions >= V3.1.39	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1243-7: All versions >= V3.1.39	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1243-7 LTE EU: All versions >=V3.1.39 and < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799604/

SIMATIC NET CP 1243-7 LTE US: All versions >=V3.1.39 and < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799604/
SIMATIC NET CP 1243-8 IRC: All versions >= V3.1.39	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1542SP-1: All versions >= V2.0	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1542SP-1 IRC (incl. SIPLUS variants): All versions >= V2.0	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1543-1 (incl. SIPLUS variants): All versions >= V2.2	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1543SP-1 (incl. SIPLUS variants): All versions >= V2.0	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1545-1: All versions	See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions < V3.0 SP1	Update to V3.0 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109793790/
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331/

WORKAROUNDS AND MITIGATIONS

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

- Where possible apply the following countermeasures:
  - Use name servers inside corporate environments
  - Restrict access of CLI and web-based management interfaces for the affected devices to a dedicated layer 2 segment/VLAN and/or controlled by firewall policies at layer 3 where possible
  - Disable outgoing ICMP packets by using “service ACLs” to implement blocking rules

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.

SIMATIC Cloud Connect 7 is an IoT Gateway to connect programmable logic controllers to cloud services and enables the connection of field devices with OPC UA server Interface as OPC UA clients.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

The SCALANCE M-800 / S615 and RUGGEDCOM RM1224 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.

The SIMATIC NET CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC NET CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1545-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

The stationary optical readers of the SIMATIC MV500 family are used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2020-25705

A flaw in ICMP packets in the Linux kernel was found to allow to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

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 (2021-05-11):	Publication Date
V1.1 (2021-06-08):	Added solution for TIM 1531 IRC
V1.2 (2021-07-13):	Added solution for SIMATIC NET CP 1243-7 LTE EU and SIMATIC NET CP 1243-7 LTE US

TERMS OF USE