SSA-324955: SAD DNS Attack in Linux Based Products

Publication Date: 2021-05-11
Last Update: 2023-03-14
Current Version: V2.0
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 the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224 family (6GK6108-4AM00): All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/ See further recommendations from section Workarounds and Mitigations
SCALANCE M-800 family: All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/ See further recommendations from section Workarounds and Mitigations
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions >= V5.0 and < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109794349/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC-600 family: All versions < V2.1.3	Update to V2.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109793041/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D: V8.3.0.1, V8.6.0 and V8.7.0	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/de/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions > V1.0 and < V1.6	Update to V1.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109803418/ See further recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions > V1.0 and < V1.6	Update to V1.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109803418/ See further recommendations from section Workarounds and Mitigations

SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions >= V3.1.39 < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799604/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions >= V3.1.39 and < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/us/en/view/109812218/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions >=V3.1.39 and < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799584/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions >=V3.1.39 and < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799584/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions >= V3.1.39 and < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/us/en/view/109812218/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 1543-1 (incl. SIPLUS variants): All versions >= V2.2 and < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109800773 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions < V1.1	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811116/ See further recommendations from section Workarounds and Mitigations

SIMATIC MV540 H (6GF3540-0GE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further recommendations from section Workarounds and Mitigations
SIMATIC MV540 S (6GF3540-0CD10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further recommendations from section Workarounds and Mitigations
SIMATIC MV550 H (6GF3550-0GE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further recommendations from section Workarounds and Mitigations
SIMATIC MV550 S (6GF3550-0CD10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further recommendations from section Workarounds and Mitigations
SIMATIC MV560 U (6GF3560-0LE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further recommendations from section Workarounds and Mitigations
SIMATIC MV560 X (6GF3560-0HE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/de/en/view/109804366 See further 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/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations

SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions >= V3.1.39 < V3.3	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799604/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions >= V3.1.39 and < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/us/en/view/109812218/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions >= V3.1.39 and < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/us/en/view/109812218/ See further recommendations from section Workarounds and Mitigations
SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions < V2.2 Update 1	Update to V2.2 Update 1 or later version https://support.industry.siemens.com/cs/de/en/view/109803672/ See further recommendations from section Workarounds and Mitigations
TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions < V2.2 Update 1	Update to V2.2 Update 1 or later version https://support.industry.siemens.com/cs/de/en/view/109803672/ See further 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:

- 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

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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.

SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 are industrial routers.

SCALANCE SC-600 devices (SC622-2C, SC626-2C, 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.

SCALANCE W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

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.

SIMATIC CP 1242-7 and CP 1243-7 LTE communications processors connect SIMATIC S7-1200 controllers to Wide Area Networks (WAN). They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1243-8 IRC communications processors connect SIMATIC S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC CP 1543-1 and SIMATIC 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.

SIMATIC CP 1243-1 communications processors connect S7-1200 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connect 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.

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

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.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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
V1.3 (2021-08-10):	Added solution for SIMATIC NET CP 1543-1
V1.4 (2021-09-14):	Errata: Removed solution for TIM 1531 IRC as V2.2 did not fix the issue
V1.5 (2021-10-12):	Corrected wrong product name SIMATIC CP 1243-7 to SIMATIC CP 1242-7 GPRS V2, updated solution for SIMATIC CP 1243-7 LTE, added solution for SIMATIC CP 1242-7 GPRS V2 and SCALANCE W1750D
V1.6 (2021-11-09):	Added solution for SIMATIC Cloud Connect 7 and TIM 1531 IRC, split TIM 1531 IRC into individual products, split SIMATIC Cloud Connect 7 into individual products
V1.7 (2021-12-14):	Added solution for the SIMATIC MV500 family products
V1.8 (2022-06-14):	Added fix for SIMATIC CP 1545-1
V1.9 (2022-08-09):	Added fix for SIMATIC CP 1243-1 and CP 1243-8 IRC
V2.0 (2023-03-14):	Added fix for SIMATIC CP 1542SP-1, SIMATIC CP 1542SP-1 IRC, and SIMATIC CP 1543SP-1

TERMS OF USE