America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Siemens PROFINET Devices (Update D)

Last Revised: April 14, 2022 **Alert Code:** ICSA-21-194-03

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Siemens
- **Equipment:** PROFINET Devices
- **Vulnerability:** Allocation of Resources Without Limits or Throttling

2. UPDATE INFORMATION

This updated advisory is a follow-up to the advisory update titled ICSA-21-194-03 Siemens PROFINET Devices (Update C) that was published October 14, 2021, to the ICS webpage on www.cisa.gov/uscert.

3. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to perform a denial-of-service attack if a large amount of PROFINET Discovery and Configuration Protocol (DCP) reset packets is sent to the affected devices.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following Siemens products are affected:

- SIMATIC PROFINET Driver: All versions prior to v2.3
- SIMATIC NET CM 1542-1: All versions prior to v3.0
- SCALANCE X204-2 (incl. SIPLUS NET variant): All versions prior to v5.2.5
- SCALANCE X204-2FM: All versions prior to v5.2.5
- SCALANCE X204-2LD (incl. SIPLUS NET variant): All versions prior to v5.2.5
- SCALANCE X20204-2LD TS: All versions prior to v5.2.5
- SCALANCE X204 -2TS: All versions prior to v5.2.5
- SCALANCE X206-1: All versions prior to v5.2.5
- SCALANCE X206-1LD (incl. SIPLUS NET variant): All versions prior to v5.2.5
- SCALANCE X208 (incl. SIPLUS NET variant): All versions prior to v5.2.5
- SCALANCE X208PRO: All versions prior to v5.2.5
- SCALANCE X212-2: All versions prior to v5.2.5

- SCALANCE X12-2LD: All versions prior to v5.2.5
- SCALANCE X216: All versions prior to v5.2.5
- SCALANCE X224: All versions prior to v5.2.5
- Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions
- Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions
- Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions
- RUGGEDCOM RM1224: All versions prior to v6.4
- SCALANCE M-800: All versions prior to v6.4
- SCALANCE S615: All versions prior to v6.4
- SCALANCE W700 IEEE 802.11n: All versions
- SCALANCE W700 IEEE 802.11ac: All versions
- SCALANCE X200-4 P IRT: All versions prior to v5.5.0
- SCALANCE X201-3P IRT: All versions prior to v5.5.0
- SCALANCE X201-3P IRT PRO: All versions prior to v5.5.0
- SCALANCE X202-2 IRT: All versions prior to v5.5.0
- SCALANCE X202-2P IRT (incl. SIPLUS NET variant): All versions prior to v5.5.0
- SCALANCE X202-2P IRT PRO: All versions prior to v5.5.0
- SCALANCE X204 IRT: All versions prior to v5.5.0
- SCALANCE X204 IRT PRO: All versions prior to v5.5.0
- SCALANCE X204-2 (incl. SIPLUS NET variant): All versions
- SCALANCE X204-2FM: All versions
- SCALANCE X204-2LD (incl. SIPLUS NET variant): All versions
- SCALANCE X20204-2LD TS: All versions
- SCALANCE X204 -2TS: All versions
- SCALANCE X206-1: All versions
- SCALANCE X206-1LD (incl. SIPLUS NET variant): All versions
- SCALANCE X208 (incl. SIPLUS NET variant): All versions

- SCALANCE X208PRO: All versions
- SCALANCE X212-2: All versions
- SCALANCE X12-2LD: All versions
- SCALANCE X216: All versions
- SCALANCE X224: All versions
- SCALANCE X302-7EEC: All versions
- SCALANCE 304-2FE: All versions

--------- Begin Update D Part 1 of 2 ---------

- SCALANCE W1748-1 M12: All versions prior to v3.0.0
- SCALANCE W1788-1 M12: All versions prior to v3.0.0
- SCALANCE W1788-2 EEC M12: All versions prior to v3.0.0
- SCALANCE W1788-2 M12: All versions prior to v3.0.0
- SCALANCE W1788-2IA M12: All versions prior to v3.0.0
- SCALANCE X302-7EEC: All versions prior to v4.1.4
- SCALANCE X306-1LDFE: All versions prior to v4.1.4
- SCALANCE X307-2EEC: All versions prior to v4.1.4
- SCALANCE X307-3: All versions prior to v4.1.4
- SCALANCE X307-3LD: All versions prior to v4.1.4
- SCALANCE X308-2 (incl. SIPLUS NET variant) All versions prior to v4.1.4
- SCALANCE X308-2LD: All versions prior to v4.1.4
- SCALANCE X308-2LH: All versions prior to v4.1.4
- SCALANCE X308-2LH+: All versions prior to v4.1.4
- SCALANCE X308-2M: All versions prior to v4.1.4
- SCALANCE X308-2M POE: All versions prior to v4.1.4
- SCALANCE X308-2M TS: All versions prior to v4.1.4
- SCALANCE X310: All versions prior to v4.1.4
- SCALANCE X310FE: All versions prior to v4.1.4

- SCALANCE X320-1FE: All versions prior to v4.1.4
- SCALANCE X320-3LDFE: All versions prior to v4.1.4
- SCALANCE X408-2: All versions prior to v4.1.4

--------- End Update D Part 1 of 2 ---------

- SCALANCE XB-200: All versions
- SCALANCE XC-200: All versions
- SCALANCE XF201-3P IRT: All versions prior to v5.5.0
- SCALANCE XF202-2P IRT: All versions prior to v5.5.0
- SCALANCE XF204: All versions
- SCALANCE XF204 IRT: All versions prior to v5.5.0
- SCALANCE XF204-2 (incl. SIPLUS NET variant): All versions
- SCALANCE XF204-2BA IRT: All versions prior to v5.5.0
- SCALANCE XF206-1: All versions
- SCALANCE XF208: All versions
- SCALANCE XF-200BA: All versions
- SCALANCE XM400: All versions prior to v6.3.1
- SCALANCE XP-200: All versions
- SCALANCE XR324-4M EEC: All versions
- SCALANCE XR324-4M POE: All versions
- SCALANCE XR324-4M POE TS: All versions
- SCALANCE XR324-12M: All versions
- SCALANCE XR324-12M TS: All versions
- SCALANCE XR500: All versions prior to v6.3.1
- SCALANCE XR-300WG: All versions
- SIMATIC CFU PA: All versions
- SIMATIC IE/PB-LINK V3: All versions
- SIMATIC MV500 family: All versions prior to v3.0

- SIMATIC NET CM 1542-1: All versions
- SIMATIC NET CP1616/CP1604: All Versions 2.7 and prior
- SIMATIC NET CP1626: All versions
- SIMATIC NET DK-16xx PN IO: All Versions 2.7 and prior
- SIMATIC Power Line Booster PLB, Base Module (MLFB: 6ES7972-5AA10-0AB0): All versions
- SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions prior to v4.5
- SIMOCODE proV Ethernet/IP: All versions prior to v1.1.3
- SIMOCODE proV PROFINET: All versions prior to v2.1.3
- SOFTNET-IE PNIO: All versions

4.2 VULNERABILITY OVERVIEW

4.2.1 ALLOCATION OF RESOURCES WITHOUT LIMITS OR THROTTLING CWE-770 <https://cwe.mitre.org/data/definitions/770.html>

Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. This vulnerability can be triggered if a large amount of DCP resent packets are sent to the device.

CVE-2020-28400 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:n/i:n/a:h>).

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Multiple
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Germany

4.4 RESEARCHER

Siemens reported this vulnerability to CISA.

5. MITIGATIONS

Siemens has provided remediations for the following affected products:

--------- Begin Update D Part 2 of 2 ---------

- SCALANCE X300 switch family: Update to v4.1.4.3 or later version
- SCALANCE X408 (incl. SIPLUS Net variants): Update to v4.1.4.3 or later version
- SCALANCE W-1700 family: Update to v3.0.0 or later version

--------- End Update D Part 2 of 2 -------

- SIMATIC NET CM 1542-1, All versions prior to v3.0: Update <https://support.industry.siemens.com/cs/ww/en/view/109801629> to v3.0 or later version
- SCALANCE X204-2 (incl. SIPLUS NET variant), All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X204-2FM, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X204-2LD (incl. SIPLUS NET variant), All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X204-2LD TS, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X204 -2TS, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X206-1, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version

- SCALANCE X206-1LD (incl. SIPLUS NET variant), All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X208 (incl. SIPLUS NET variant), All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X208PRO, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X212-2, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X212-2LD, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X216, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- SCALANCE X224, All versions: Update <https://support.industry.siemens.com/cs/ww/en/view/109801131> to v5.2.5 or later version
- Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: Update <https://support.industry.siemens.com/cs/ww/en/view/109784253/> to v4.7or later version
- SCALANCE XR-300WG, All versions prior to v4.3: Update to v4.3 or later version
- SCALANCE XB-200, All versions prior to v4.3: Update to v4.3 or later version
- SCALANCE XP-200, All versions prior to v4.3: Update to v4.3 or later version
- SCALANCE XC-200, All versions prior to v4.3: Update to v4.3 or later version
- SCALANCE XF-200BA, All versions prior to v4.3: Update to v4.3 or later version
- RUGGEDCOM RM1224, All versions prior to v6.4: Update <http://support.automation.siemens.com/ww/view/en/109794349> to v6.4 or later version
- SCALANCE M-800, All versions prior to v6.4: Update <http://support.automation.siemens.com/ww/view/en/109794349> to v6.4 or later version
- SCALANCE S615, All versions prior to v6.4: Update <http://support.automation.siemens.com/ww/view/en/109794349> to v6.4 or later version
- SCALANCE X200-4 P IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version

- SCALANCE X201-3P IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X201-3P IRT PRO, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X202-2 IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X202-2P IRT (incl. SIPLUS NET variant), All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X202-2P IRT PRO, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X204 IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE X204 IRT PRO, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE XF201-3P IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE XF202-2P IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE XF204 IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE XF204-2BA IRT, All versions prior to v5.5.0: Update <http://support.automation.siemens.com/ww/view/en/109793952> to v5.5.0 or later version
- SCALANCE XM400, All versions prior to v6.3.1: Update <http://support.automation.siemens.com/ww/view/en/109782067> to v6.3.1 or later version
- SCALANCE XR500, All versions prior to v6.3.1: Update <http://support.automation.siemens.com/ww/view/en/109782065> to v6.3.1 or later version
- SIMATIC MV500 family, All versions prior to v3.0: Update <http://support.automation.siemens.com/ww/view/en/109795469> to v3.0 or later version

- SIMATIC S7-1200 CPU family (incl. SIPLUS variants), All versions prior to v4.5: Update <http://support.automation.siemens.com/ww/view/en/109793280> to v4.5 or later version
- SIMOCODE proV Ethernet/IP, All versions prior to v1.1.3: Update <http://support.automation.siemens.com/ww/view/en/109756912> to v1.1.3 or later version
- SIMOCODE proV PROFINET, All versions prior to v2.1.3: Update <http://support.automation.siemens.com/ww/view/en/109749989> to v2.1.3 or later version

Siemens has also identified the following specific workarounds and mitigations users can apply to reduce the risk:

- Block incoming PROFINET Discovery and Configuration Protocol (PCP) packets (Ethertype 0x8892, Frame-ID: 0xfefe) from untrusted networks.
- Disable PROFINET in products, where PROFINET is optional and not used in the environment.

As a general security measure, Siemens strongly recommends protecting network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for Industrial Security <http://support.automation.siemens.com/ww/view/en/109749989>, 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 <https://www.siemens.com/industrialsecurity>

For more information about this vulnerability and the associated remediations, please see Siemens publication number SSA-599968 <https://cert-portal.siemens.com/productcert/pdf/ssa-599968.pdf>

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet <https://us-cert.cisa.gov/ics/alerts/ics-alert-10-301-01>.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://us-cert.cisa.gov/ics/recommended-practices> on the ICS webpage on us-cert.cisa.gov <https://us-cert.cisa.gov/ics>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov <https://us-cert.cisa.gov/ics> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://us-cert.cisa.gov/ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Siemens

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov