# SSA-349422: Denial of Service Vulnerability in Industrial Real-Time (IRT) Devices

Publication Date: 2019-10-08
Last Update: 2025-02-11
Current Version: V2.2
CVSS v3.1 Base Score: 7.5

## SUMMARY

A vulnerability in the affected products could allow an unauthorized attacker with network access to perform a denial-of-service attack resulting in loss of real-time synchronization.

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

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller: All versions < V4.1.1 Patch 05 affected by CVE-2019-10923 | Update to V4.1.1 Patch 05 or later version https://support.industry.siemens.com/cs/ww/en/view/109755160/ See further recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: All versions < V4.5.0 Patch 01 affected by CVE-2019-10923 | Update to V4.5.0 Patch 01 or later version https://support.industry.siemens.com/cs/ww/en/view/109760397/ See further recommendations from section Workarounds and Mitigations |
| Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: All versions < V4.5.0 affected by CVE-2019-10923 | Update to V4.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109750012/ See further recommendations from section Workarounds and Mitigations |
| SCALANCE X-200IRT family (incl. SIPLUS NET variants): All versions < V5.2.1 affected by CVE-2019-10923 | Update to V5.4.2 https://support.industry.siemens.com/cs/ww/en/view/109763309 See further recommendations from section Workarounds and Mitigations |
| SIMATIC CP 1604 (6GK1160-4AA01): All versions < V2.8 affected by CVE-2019-10923 | Update to V2.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109762689/ See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC CP 1616 (6GK1161-6AA02):<br>All versions < V2.8<br>affected by CVE-2019-10923 | Update to V2.8<br>https://support.industry.siemens.com/cs/ww/en/view/109762689/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN: | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12 (6ES7141-6BH00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12 (6ES7142-6BH00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 4AO U/I 4xM12 (6ES7145-6HD00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8 DIO, DC24V/1,3A, 8xM12 (6ES7147-6BG00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12 (6ES7142-6BR00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12 (6ES7144-6KD50-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8AI; 4 U/I; 4 RTD/TC 8xM12 (6ES7144-6KD00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12 (6ES7141-6BF00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12 (6ES7141-6BG00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12 (6ES7142-6BF50-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12 (6ES7142-6BF00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12 (6ES7142-6BG00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200ecoPN: IO-Link Master (6ES7148-6JA00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET200S (incl. SIPLUS variants):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200M (incl. SIPLUS variants):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200MP IM 155-5 PN HF (incl. SIPLUS variants): | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/93012181/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200MP IM 155-5 PN HF (6ES7155-5AA00-0AC0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/93012181/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/93012181/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/93012181/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/93012181/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ET 200MP IM 155-5 PN ST (incl. SIPLUS variants): | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78647504/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200MP IM 155-5 PN ST (-Ax00) (incl. SIPLUS variants): | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78647504/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200MP IM 155-5 PN ST (6ES7155-5AA00-0AB0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78647504/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200MP IM 155-5 PN ST (6AG1155-5AA00-7AB0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78647504/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200MP IM 155-5 PN ST TX RAIL (6AG2155-5AA00-4AB0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78647504/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200pro IM 154-3 PN HF (6ES7154-3AB00-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200pro IM 154-4 PN HF (6ES7154-4AB10-0AB0):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200pro IM 154-8 PN/DP CPU (6ES7154-8AB01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47354502/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200pro IM 154-8F PN/DP CPU (6ES7154-8FB01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47354578/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ET 200pro IM 154-8FX PN/DP CPU (6ES7154-8FX00-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/62612377/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200S IM 151-8 PN/DP CPU (6ES7151-8AB01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47353723/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200S IM 151-8F PN/DP CPU (6ES7151-8FB01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47354354/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants): | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85624387/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200SP IM 155-6 PN HF (6ES7155-6AU00-0CN0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85624387/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-4CN0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85624387/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU00-2CN0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85624387/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU00-1CN0):<br>All versions < V4.2.0<br>affected by CVE-2019-10923 | Update to V4.2.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85624387/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC ET 200SP IM 155-6 PN ST (incl. SIPLUS variants): | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200SP IM 155-6 PN ST (-Ax00) (incl. SIPLUS variants): | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200SP IM 155-6 PN ST (6ES7155-6AU00-0BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC ET 200SP IM 155-6 PN ST BA (6ES7155-6AA00-0BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN ST (6AG1155-6AU00-7BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN ST BA (6AG1155-6AA00-7BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN ST BA TX RAIL (6AG2155-6AA00-4BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP IM 155-6 PN ST TX RAIL (6AG2155-6AU00-4BN0):<br>All versions < V4.1.0<br>affected by CVE-2019-10923 | Update to V4.1.0 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/78648144/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC PN/PN Coupler (incl. SIPLUS NET variants):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/51466769/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40360647/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40944925/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85049260/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40362228/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40945128/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85059804/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/85063017/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/44442927/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/44443101/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants):<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0):<br>All versions < V2010 SP3<br>affected by CVE-2019-10923 | Update to V2010 SP3 or later version and apply BIOS and Microsoft Windows updates<br>https://support.industry.siemens.com/cs/ww/en/view/109765109/<br>See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0):<br>All versions < V2010 SP3<br>affected by CVE-2019-10923 | Update to V2010 SP3 or later version and apply BIOS and Microsoft Windows updates<br>https://support.industry.siemens.com/cs/ww/en/view/109765109/<br>See further recommendations from section Workarounds and Mitigations |
| SIMOTION:<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SINAMICS DCM:<br>All versions < V1.5 HF1<br>affected by CVE-2019-10923 | Update to V1.5 HF1 or later version<br>https://support.industry.siemens.com/cs/us/en/view/44029688<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS DCP:<br>All versions < V1.3<br>affected by CVE-2019-10923 | Update to V1.3<br>https://support.industry.siemens.com/cs/ww/de/view/109773826<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS G110M V4.7 Control Unit:<br>All versions < V4.7 SP10 HF5<br>affected by CVE-2019-10923 | Update to V4.7 SP10 HF5<br>https://support.industry.siemens.com/cs/us/en/view/109756820<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS G120 V4.7 Control Unit (incl. SIPLUS variants):<br>All versions < V4.7 SP10 HF5<br>affected by CVE-2019-10923 | Update to V4.7 SP10 HF5<br>https://support.industry.siemens.com/cs/us/en/view/109756820<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS G130/G150/S150 family: | Update to V4.7 HF29 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/103433117/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SINAMICS G130:<br>All versions < V4.7 HF29<br>affected by CVE-2019-10923 | Update to V4.7 HF29 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/103433117/<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS G150:<br>All versions < V4.7 HF29<br>affected by CVE-2019-10923 | Update to V4.7 HF29 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/103433117/<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS S150:<br>All versions < V4.7 HF29<br>affected by CVE-2019-10923 | Update to V4.7 HF29 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/103433117/<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS GH150 V4.7 Control Unit:<br>All versions<br>affected by CVE-2019-10923 | Update to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS GL150 V4.7 Control Unit:<br>All versions<br>affected by CVE-2019-10923 | Update to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS GM150 V4.7 Control Unit:<br>All versions<br>affected by CVE-2019-10923 | Update to V4.8 SP2 HF9<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS S110 Control Unit:<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SINAMICS S120 V4.7 Control Unit and CBE20 (incl. SIPLUS variants):<br>All versions < V4.7 HF34<br>affected by CVE-2019-10923 | Update to V4.7 HF34 or upgrade to V5.2 HF2<br>https://support.industry.siemens.com/cs/us/en/view/92522512<br>See further recommendations from section Workarounds and Mitigations |
| SINAMICS SL150 V4.7 Control Unit:<br>All versions < V4.7 HF33<br>affected by CVE-2019-10923 | Update to V4.7 HF33<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SINAMICS SM120 V4.7 Control Unit:<br>All versions<br>affected by CVE-2019-10923 | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SINUMERIK 828D:<br>All versions < V4.8 SP5<br>affected by CVE-2019-10923 | Update to V4.8 SP5 or later version<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |
| SINUMERIK 840D sl:<br>All versions < V4.8 SP5<br>affected by CVE-2019-10923 | Update to V4.8 SP5 or later version<br>The update can be obtained from your Siemens representative or via Siemens customer service.<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200S IM 151-8 PN/DP CPU (6AG1151-8AB01-7AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47353723/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200S IM 151-8F PN/DP CPU (6AG1151-8FB01-2AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/47354354/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0):<br>All versions < V3.3.17<br>affected by CVE-2019-10923 | Update to V3.3.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/51466769/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40360647/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40944925/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40362228/<br>See further recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0):<br>All versions < V3.2.17<br>affected by CVE-2019-10923 | Update to V3.2.17 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/40945128/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>See further recommendations from section Workarounds and Mitigations |
| SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0):<br>All versions < V7.0.3<br>affected by CVE-2019-10923 | Update to V7.0.3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109752685/<br>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:

- Disable SNMP in Versions 1 and 2c, if supported by the product.
- Enable SNMP v3 if required and supported by the product to restrict the vulnerability to authenticated users.
- Enable access protection and change default credentials for SNMP service, if possible
- Restrict network access to port 161/udp of the affected product.

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

Development/Evaluation Kits for PROFINET IO are used to develop compact or modular PROFINET field devices.

PN/PN coupler is used for connecting two PROFINET networks.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIMATIC CP 1604 and CP 1616 are PCI/PCI-104 cards for high-performance connection of field devices to Industrial Ethernet with PROFINET.

SIMATIC ET 200 Interface modules for PROFINET IO are used to connect field devices (IO Devices) to controllers (IO Controller) via PROFINET.

SIMATIC S7-300 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-400 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

SIMOTION is a scalable high performance hardware and software system for motion control.

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.

## VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### Vulnerability CVE-2019-10923

An attacker with network access to an affected product may cause a denial of service condition by breaking the real-time synchronization (IRT) of the affected installation.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-400: Uncontrolled Resource Consumption |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

## 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 (2019-10-08): | Publication Date |
| V1.1 (2020-01-14): | Added solution for SINAMICS SL150 V4.7, SIPLUS devices now explicitly mentioned in the list of affected products, correction in section "Workarounds and Mitigations" |
| V1.2 (2020-02-11): | Added solution for SINAMICS DCP |
| V1.3 (2020-03-10): | Added solution for SIMATIC S7-300 CPU family |
| V1.4 (2020-08-11): | Added SIMATIC ET200ecoPN product variants (MLFB IDs) that are not affected |
| V1.5 (2021-02-09): | Added additional SIMATIC ET200ecoPN model (6ES7148-6JG00-0BB0) as not affected |
| V1.6 (2021-10-12): | Clarified affected ET200ecoPN models |
| V1.7 (2022-02-08): | Clarified that no remediation is planned for ET200 devices |
| V1.8 (2023-01-10): | SIMATIC S7-300 CPU family expanded with product specific designations, patch links and MLFBs. Added fix for SINUMERIK 840D sl. |

V1.9 (2023-04-11): SIMATIC S7-400 CPU family expanded and fix added for supported versions, no fix planned for other S7-400 versions
V2.0 (2023-05-09): Removed SIMATIC S7-400 CPU devices without fix, as they do not support PROFINET and are not affected
V2.1 (2024-09-10): Listed affected products individually instead of product families (e.g., for SIMATIC ET 200AL/MP/SP/pro IM families); added affected SIPLUS devices (e.g., SIPLUS ET 200xx IM)
V2.2 (2025-02-11): Added fix for SINAMICS G150 and SINAMICS S150

## TERMS OF USE