**CSAF: 62c3f0a599cf2533865817cd**

The attacker must have network access to the local Ethernet segment (Layer 2).. Siemens provides firmware updates fixing these vulnerabilities for the following affected products and recommends users update to the new fixed version:. Development/Evaluation Kits DK Standard Ethernet Controller: Update to v4.1.1 Patch04. Development/Evaluation Kits EK-ERTEC 200P PN IO: Update to v4.4.0 Patch01. Development/Evaluation Kits EK-ERTEC 200 PN IO: Update to v4.2.1 Patch03. IE/PB-Link: Update to v3.0. SCALANCE M-800, S615: Update to v04.3. SCALANCE W700: Update to v6.1.0. SCALANCE X-300/X408: Update to v4.1.0. SCALANCE X414: Update to v3.10.2. SCALANCE X-200: Update to v5.2.2. SCALANCE X-200IRT: Update to v5.4.0. SCALANCE XM-400: Update to v6.1. SCALANCE XR-500: Update to v6.1. SIMATIC DK-16xx PN IO: Update to v2.7. SIMATIC ET 200AL: Update to v1.0.2. SIMATIC ET 200MP IM155-5 PN BA: Update to v4.0.1 or newer. SIMATIC ET 200MP IM155-5 PN HF: Update to v4.2. SIMATIC ET 200MP IM155-5 PN ST: Update to v4.1 --------- Begin Update V Part 1 of 1 ---------. SIMATIC ET 200SP: No remediation is currently planned --------- End Update V Part 1 of 1 ---------. SIMATIC ET 200SP IM155-6 PN HF: Update to v4.2.0. SIMATIC ET 200SP IM155-6 PN HS: Update to v4.0.1. SIMATIC ET 200SP IM155-6 PN ST: Update to v4.1.0. SIMATIC HMI Comfort Panels, HMI Multi Panels, HMI Mobile Panels: Update to v15.1. SIMATIC MV400 family: Update to v7.0.6. SIMATIC NET CM 1542-1: Update to v2.0. SIMATIC NET CM 1542SP-1: Update to v1.0.15. SIMATIC NET CP 343-1 Std and SIMATIC NET CP 343-1 Lean: Update to v3.1.3. SIMATIC NET CP 443-1 Advanced: Update to v3.2.17. SIMATIC NET CP 443-1 Standard: Update to v3.2.17. SIMATIC NET CP 1243-1 and SIMATIC NET CP 1243-1 IRC: Update to v3.1. SIMATIC NET CP 1542SP-1, CP 1542SP-1 IRC, and CP 1543SP-1: Update to v1.0.15. SIMATIC NET CP 1543-1: Update to v2.1. SIMATIC NET CP 1604, 1616: Update to v2.8.0. SIMATIC PN/PN Coupler: Update to v4.0. SIMATIC RF650R, RF680R, RF685R: Update to v3.0. SIMATIC S7-200 SMART: Contact a Siemens representative or customer support to update to v2.3. SIMATIC S7-300 CPU family: Update to v3.X.14. SIMATIC S7-400 H V6 CPU family: Update to v6.0.7. SIMATIC S7-400 PN/DP V6 CPU family: Update to v6.0.6. SIMATIC S7-400 PN/DP V7 CPU family: Update to v7.0.2. SIMATIC S7-410 CPU family: Update to v8.2. SIMATIC S7-1200 including F: Update to v4.2.1. SIMATIC S7-1500 including F, T and TF: Update to v2.1. SIMATIC S7-1500 Software Controller including F: Update to v2.1. SIMATIC TDC CP51M1: Update to v1.1.8. SIMATIC TDC CPU555: Update to v1.1.1. SIMATIC Teleservice Adapters (IE Basic, IE Standard, IE Advanced): migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation.. SIMATIC WinAC RTX (F) 2010: Update to SIMATIC WinAC RTX 2010 SP3 and apply BIOS and Microsoft Windows updates. SIMOCODE pro V PN: Update to v2.0.0. SIMOTION: Update to v4.5 HF1. SINAMICS DCM w. PN: Update to v1.4 SP1 HF5. SINAMICS DCP w. PN: Update to v1.2 HF1. SINAMICS G110M/G120(C/P/D) w. PN: Update to v4.7 SP6 HF3. SINAMICS G130 and G150 v4.7: Update to v4.7 HF27. SINAMICS G130 and G150 v4.8: Update to v4.8 HF4. SINAMICS S110 w. PN: Update to v4.4 SP3 HF5. SINAMICS S120 v4.7: Update to v4.7 HF27. SINAMICS S120 v4.8: Update to v4.8 HF4. SINAMICS S150 v4.7: Update to v4.7 HF27. SINAMICS S150: v4.8: Update to v4.8 HF4. SINAMICS v90 w. PN: Update to v1.1. SINUMERIK 828D v4.5: Update to v4.5 SP6 HF2. SINUMERIK 828D v4.7: Update to v4.7 SP4 HF1. SINUMERIK 840D sl v4.5 and prior: Update to v4.5 SP6 HF8. SINUMERIK 840D sl v4.7: Update to v4.7 SP4 HF1 SINUMERIK software updates listed above can be obtained from a Siemens account manager.. SIRIUS ACT 3SU1 interface module PROFINET: Update to v1.1.0. SITOP PSU8600 PROFINET: Update to v1.2.0. SITOP UPS1600 PROFINET: Update to v2.2.0. Softnet PROFINET IO for PC-based Windows systems: Update to v14 SP1 Siemens is preparing updates for the remaining affected products and recommends the following mitigations in the meantime:. Apply cell protection concept.. Use VPN for protecting network communication between cells.. Apply defense-in-depth. As a general security measure Siemens strongly recommends protecting industrial control systems networks with appropriate mechanisms. Siemens strongly recommends verifying the affected products are protected as described in PROFINET Security Guidelines and Siemens Operational Guidelines in order to run the devices in a protected IT environment.. For more information on these vulnerabilities and more detailed mitigation instructions, please see Siemens Security Advisory SSA-293562. 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 these vulnerabilities. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a599cf2533865817a4**

Siemens recommends updating the following products to the most current BIOS version where available:. SIMATIC Field PG M5: Update BIOS to v22.01.08. SIMATIC Field PG M6: Update BIOS to v26.01.07. SIMATIC IPC427E, IPC477E, IPC477E Pro: Update BIOS to v21.01.14. SIMATIC IPC527G: Update BIOS to R1.4.0. SIMATIC IPC547G: Update BIOS to R1.28.0. SIMATIC IPC627E, IPC647E, IPC677E, and IPC847E: Update BIOS to v25.02.06. SIMATIC ITP1000: Update BIOS to v23.01.08 --------- Begin Update F Part 2 of 2 ---------. SIMATIC IPC3000 SMART v2: Update BIOS to v1.B or later version --------- End Update F Part 2 of 2 ---------. Siemens is preparing further updates and recommends the following specific workarounds and mitigations users can apply to reduce the risk until fixes are available.. As a prerequisite for an attack, an attacker must be able to run untrusted code on affected systems. Siemens recommends limiting the possibilities to run untrusted code if possible.. Applying a defense-in-depth concept can help to reduce the probability that untrusted code is run on the system. Siemens recommends applying the defense-in-depth concept. 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, and following the recommendations in the product manuals.. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/Industrialsecurity. For more information on these vulnerabilities and the associated mitigations, please see Siemens security advisory SSA-534763. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. 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 on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 vulnerability is not exploitable remotely. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a599cf25338658177b**

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available:. SIMATIC Drive Controller family: Update to v2.9.4 or later version. SIMATIC S7-1200 CPU family: Update to v4.5.2 or later version. SIMATIC S7-1500 CPU family: Update to v2.9.4 or later version ------- Begin Update A Part 2 of 2 -------. SIMATIC s7-PLCSIM Advanced: Update to v4.0 SP1 or later version ------- End Update A Part 2 of 2 -------. As a general security measure, Siemens strongly recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens’ operational guidelines for industrial security, and following the recommendations in the product manuals. . Additional information on industrial security by Siemens can be found at: https://www.siemens.com/industrialsecurity. For more information see Siemens Security Advisory SSA-838121. CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:. Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 these vulnerabilities. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a599cf253386581752**

Siemens has released updates for the affected products and recommends updating to the latest versions.. SINUMERIK MC: Update to v1.15 SP1 or later versions. SINUMERIK ONE: Update to v6.15 SP1 or later versions SINUMERIK software can be obtained from a Siemens account manager.. 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, 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. For additional information, please refer to Siemens Security Advisory SSA-337210. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 vulnerability is not exploitable remotely. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a599cf253386581729**

Siemens currently has updates for the following products:. SIMATIC ET 200 Open Controller CPU 1515SP PC2: Update to v2.7. SIMATIC HMI Comfort Outdoor Panels 7" & 15" (including SIPLUS variants): Update to v15.1 Upd 4. SIMATIC HMI Comfort Panels 4" 22" (including SIPLUS variants): Update to v15.1 Upd 4. SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900, KTP900F (including SIPLUS variants): Update to v15.1 Upd 4. SIMATIC IPC DiagMonitor: Update to v5.1.3 --------- Begin Update G Part 2 of 2 ----------. SIMATIC NET PC Software v14: Update to v14 SP1 Update 14 or later version --------- End Update G Part 2 of 2 ----------. SIMATIC RF188C: Update to v1.1.0. SIMATIC RF600R: Update to v3.2.1. SIMATIC S7-1500 CPU Family (including related ET200 CPUs and SIPLUS variants): Update to v2.6.1. SIMATIC S7-1500 Software Controller: Update to v2.7. SIMATIC WinCC OA: Update to v3.15-P018 (logon required). SIMATIC WinCC Runtime Advanced: Update to v15.1 Upd 4. SINEC-NMS: Update to v1.0 SP1. SINEMA Server: Update to v14 SP2. SINUMERIK OPC UA Server: Update to v2.1 or newer For the balance of the listed products, Siemens is preparing further updates and recommends users apply the following specific workarounds and mitigations to reduce risk until patches are available:. Deactivate the OPC UA Service if supported by the product.. Apply cell protection concept.. Use VPN for protecting network communication between cells.. Apply Defense-in-Depth. Siemens recommends users configure their environment according to Siemens’ operational guidelines for Industrial Security (Download) and follow the recommendations in the product manuals.. Additional information on industrial security by Siemens can be found at: https://www.siemens.com/industrialsecurity. For more information on the vulnerability and more detailed mitigation instructions, please see Siemens Security Advisory SSA-307392. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CASF: 62c3f0a599cf253386581700**

Siemens has released updates for the following affected products and recommends users update to the new version:. SIMATIC WinCC Runtime Advanced: update to v16. SIMATIC WinCC Runtime Professional: update to v16 --------- Begin Update C Part 2 of 2 --------. SIMATIC NET PC Software v14: Update to v14 SP1 Update 14 or later version --------- End Update C Part 2 of 2 --------. SIMATIC STEP 7 (TIA Portal): update to v16. SIMATIC WinCC (TIA Portal): update to v16. SIMATIC WinCC OA: update to v3.16 patch 13. TIM 1531 IRC (incl. SIPLUS NET variants): update to v2.1 Siemens is preparing further updates and recommends users apply the following specific countermeasures to reduce the risk until additional patches are available:. Apply defense-in-depth As a general security measure, Siemens strongly recommends protecting network access to devices with appropriate mechanisms. Siemens recommends users configure their environment according to the Siemens Operational Guidelines for Industrial Security and follow the recommendations in the product manuals to operate the devices in a protected environment.. Additional information on industrial security by Siemens can be found at: https://www.siemens.com/industrialsecurity. For further inquiries on security vulnerabilities in Siemens products, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories. For more information on the vulnerability and more detailed mitigation instructions, please see Siemens Security Advisory SSA-273799. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:. Ensure that control system equipment is physically protected (e.g., in locked control panels).. Implement physical access control to areas in which control system devices are located. 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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. High skill level is required to exploit this vulnerability. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a599cf2533865816d7**

Siemens has released updates for the following affected products and is working on further updates. For the remaining affected products, Siemens recommends specific countermeasures until fixes are available:. SIMATIC NET PC software: Update to v16 Upd3. SIMATIC PCS neo: Update to v3.0 SP1 (Contact your local support to obtain update software). SIMATIC S7-1500 Software Controller: Update to v21.8. SIMATIC STEP 7: Update to v5.6 SP2 HF3. SIMATIC STEP 7 (TIA Portal) v13: Update to v13 SP2 Update 4. SIMATIC STEP 7 (TIA Portal) v15: Update to v15.1 Update 5. SIMATIC STEP 7 (TIA Portal) v16: Update to v16 Update 2. SIMATIC WinCC OA v3.16: Update to v3.15-P018 or newer. SIMATIC WinCC OA v3.17: Update to v3.17-P003 or newer. SIMATIC WinCC Runtime Advanced: Update to v16 Update 2. SIMATIC WinCC Runtime Professional v13: Update to v13 SP2 Update 4. SIMATIC WinCC Runtime Professional v15: Update to v15.1 Update 5. SIMATIC WinCC Runtime Professional v16: Update to v16 Update 2. SIMATIC WinCC v7.4: Update to v7.4 SP1 Update 14. SIMATIC WinCC v7.5: Update to v7.5 SP1 Update 3. SINAMICS STARTER: Update to v5.4 HF2. SINAMICS Startdrive: Update to v16 Update 3. SINEC NMS: Install provided patch. SINEMA Server: Install provided patch. SIMATIC STEP 7 (TIA Portal) v14: Update to v14 SP1 Update 10. SIMATIC WinCC Runtime Professional v14: Update to v14 SP1 Update 10. SINUMERIK ONE virtual: Update to v6.14 (Update can be obtained from Siemens Customer Service). SINUMERIK Operate: Update to v6.14 (Update can be obtained from Siemens Customer Service). SIMATIC Automation Tool: Update to v4 SP2 or newer. SINEC NMS: Update to v1.0 SP2. SINEMA Server: Update to v14 SP3 or later. SIMATIC ProSave: Update to v17 or later. NOTE: Some versions of SIMATIC ProSave are not available as separate download (e.g., v17). In this case, use the version of SIMATIC ProSave as bundled with the corresponding version of SIMATIC WinCC (TIA Portal).. --------- Begin Update J Part 2 of 2 ---------. SIMATIC NET PC software 14: Update to v14 SP1 Update 14 or later. SIMATIC NET PC software 15: Currently no fix planned. SIMATIC NET PC software 16: Update to v16 Upd3 or later --------- End Update J Part 2 of 2 ---------. Siemens has identified the following specific workarounds and mitigations that can be applied to reduce the risk:. Ensure there is no executable at the following locations:. C:\Program.exe. C:\Program Files\Common.exe. C:\Program Files\Common Files\Siemens\Automation\Simatic.exe. . Deactivate the Windows service called TraceConceptX. This leads to loss of tracing functionality and should only be considered a temporary workaround. 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 the Siemens operational guidelines for Industrial Security and following the recommendations in the product manuals.. For additional information, please refer to Siemens Security Advisory SSA-312271. 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.. 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.. This vulnerability is not exploitable remotely. No known public exploits specifically target this vulnerability. This product is provided subject to this Notification and this Privacy & Use policy.

**CASF: 62c3f0a599cf2533865816ae**

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 to v3.0 or later version. SCALANCE X204-2 (incl. SIPLUS NET variant), All versions: Update to v5.2.5 or later version. SCALANCE X204-2FM, All versions: Update to v5.2.5 or later version. SCALANCE X204-2LD (incl. SIPLUS NET variant), All versions: Update to v5.2.5 or later version. SCALANCE X204-2LD TS, All versions: Update to v5.2.5 or later version. SCALANCE X204 -2TS, All versions: Update to v5.2.5 or later version. SCALANCE X206-1, All versions: Update to v5.2.5 or later version. SCALANCE X206-1LD (incl. SIPLUS NET variant), All versions: Update to v5.2.5 or later version. SCALANCE X208 (incl. SIPLUS NET variant), All versions: Update to v5.2.5 or later version. SCALANCE X208PRO, All versions: Update to v5.2.5 or later version. SCALANCE X212-2, All versions: Update to v5.2.5 or later version. SCALANCE X212-2LD, All versions: Update to v5.2.5 or later version. SCALANCE X216, All versions: Update to v5.2.5 or later version. SCALANCE X224, All versions: Update to v5.2.5 or later version. Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: Update 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 to v6.4 or later version. SCALANCE M-800, All versions prior to v6.4: Update to v6.4 or later version. SCALANCE S615, All versions prior to v6.4: Update to v6.4 or later version. SCALANCE X200-4 P IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X201-3P IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X201-3P IRT PRO, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X202-2 IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X202-2P IRT (incl. SIPLUS NET variant), All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X202-2P IRT PRO, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X204 IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE X204 IRT PRO, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE XF201-3P IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE XF202-2P IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE XF204 IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE XF204-2BA IRT, All versions prior to v5.5.0: Update to v5.5.0 or later version. SCALANCE XM400, All versions prior to v6.3.1: Update to v6.3.1 or later version. SCALANCE XR500, All versions prior to v6.3.1: Update to v6.3.1 or later version. SIMATIC MV500 family, All versions prior to v3.0: Update to v3.0 or later version. SIMATIC S7-1200 CPU family (incl. SIPLUS variants), All versions prior to v4.5: Update to v4.5 or later version . SIMOCODE proV Ethernet/IP, All versions prior to v1.1.3: Update to v1.1.3 or later version. SIMOCODE proV PROFINET, All versions prior to v2.1.3: Update 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, 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 . For more information about this vulnerability and the associated remediations, please see Siemens publication number SSA-599968. 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.. 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 on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a599cf253386581685**

Siemens recommends updating to the latest software version:. SIMATIC IPC627E: Update BIOS to v25.02.10. SIMATIC IPC647E: Update BIOS to v25.02.10. SIMATIC IPC677E: Update BIOS to v25.02.10. SIMATIC IPC847E: Update BIOS to v25.02.10. SINUMERIK One NCU 1740: Update BIOS to v05.00.00.00 or later (Obtained through a Siemens account manager). SIMATIC IPC127E: Update BIOS to v21.01.07 or later. SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): Update BIOS to v0209\_0105 or later --------- Begin Update C Part 2 of 2 ---------. • SIMATIC IPC427E: Update BIOS to v21.01.16 or later • SIMATIC IPC477E: Update BIOS to v21.01.16 or later • SIMATIC IPC477E Pro: Update BIOS to v21.01.16 or later. --------- End Update C Part 2 of 2 ---------. 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 users configure the environment according to the Siemens operational guidelines for industrial security and follow the recommendations in the product manuals.. For additional information, please refer to Siemens Security Advisory SSA-309571. CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:. Ensure the least-privilege user principle is followed. 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.. CISA also recommends users take the following measures to protect themselves from social engineering attacks:. Do not click web links or open unsolicited attachments in email messages.. Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.. Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks. No known public exploits specifically target these vulnerabilities. These vulnerabilities are not exploitable remotely. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf25338658165c**

Siemens recommends updating their software to the latest version:. SIMATIC STEP 7 (TIA Portal) v15: Currently no fix is planned. SIMATIC STEP 7 (TIA Portal) v16: Update to v16 Update 5 or later. SIMATIC STEP 7 (TIA Portal) v17: Update to v17 Update 2 or later Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:. Whenever changes of the web server’s user configuration are performed with one of the affected versions for S7-1200 or S7-1500 CPUs (incl. related ET200 CPUs and SIPLUS variants), validate web server permissions for unauthenticated users by directly accessing the web server in an unauthenticated manner. If unintentional, unauthenticated access is possible, the web server’s user configuration needs to be removed and reconfigured using TIA-Portal v16 Update 5 or later, or v17 Update 2 or later. If a new TIA-Portal version is not available, updating the web server’s user configuration is not effective.. The PLC must be deleted and reconfigured with a new project. Warning: Copy the PLC-program before deleting the PLC or use the original project (one that was not uploaded by a PLC) to update the web server’s user management and to download the changed configuration 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 users configure the environment according to the Siemens operational guidelines for industrial security and follow the recommendations in the product manuals.. For additional information, please refer to Siemens Security Advisory SSA-350757. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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.. CISA also recommends users take the following measures to protect themselves from social engineering attacks:. Do not click web links or open unsolicited attachments in email messages.. Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.. Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks. No known public exploits specifically target this vulnerability. This vulnerability is not exploitable remotely. This vulnerability has a high attack complexity. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf253386581633**

Siemens is working on an update for the latest firmware version, and recommends the following mitigations:. Apply defense-in-depth.. Only build and run applications from trusted sources. For more information about these vulnerabilities and the associated mitigations, please see SSB-439005. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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.. CISA also recommends users take the following measures to protect themselves from social engineering attacks:. Do not click web links or open unsolicited attachments in email messages.. Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.. Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks. No known public exploits specifically target these vulnerabilities. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf25338658160a**

Siemens recommends updating their software to the most current version where available:. SIMATIC S7-400 HV6 CPU family (incl. SIPLUS variants): Update to v6.0.10 or later. SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): No current fix is available. SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): No current fix is available. SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants): Update to v10.1 or later. To obtain SIMATIC S7-410 v10.1 contact your local support. Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:. Limit access to Port 102/TCP to trusted users and systems only 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 the Siemens operational guidelines for industrial security and following the recommendations in the product manuals.. For additional information, please refer to Siemens Security Advisory SSA-557541. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a499cf2533865815e1**

Siemens recommends users follow the specific workarounds and mitigations below. Siemens has also released fixes for the following products:. CloudConnect 712: Update to v1.1.5. ROX II: Update to v2.13.3 (Only vulnerable to CVE-2019-11479). RUGGEDCOM APE 1404 Linux: Apply the latest available Debian patches. RUGGEDCOM RM1224: Update to v6.2 or later. RUGGEDCOM RX1400 VPE Debian Linux: Apply the latest available Debian patches in the VPE. RUGGEDCOM RX1400 VPE Linux CloudConnect: Apply the latest available Debian patches in the VPE or apply the latest CloudConnect VPE Linux image. SCALANCE M804PB, SCALANCE M812-1 ADSL-Router, SCALANCE M816-1 ADSL-Router, SCALANCE M826-2 SHDSL-Router, SCALANCE M874-2, SCALANCE M874-3, SCALANCE M876-3, SCALANCE M876-4, SCALANCE S615: Update to v6.2 or later. SCALANCE M875: Upgrade hardware to SCALANCE M876-4 or RUGGEDCOM RM1224 and apply patches when available. SCALANCE S602, SCALANCE S612, SCALANCE S623, SCALANCE S627-2M: Update to v4.1, Upgrade hardware to successor product from SCALANCE SC-600 family. SCALANCE SC622-2C, SCALANCE SC632-2C, SCALANCE SC636-2C, SCALANCE SC642-2C, SCALANCE SC646-2C: Update to v2.0.1. SCALANCE W1750D: Update to v8.6.0 or later versions. SCALANCE W700 IEEE 802.11n family: Update to v6.4 or newer versions --------- Begin Update R Part 2 of 2 ---------. SIMATIC CP 442-1 RNA: Update to v1.5.18 or later versions. SIMATIC CP 443-1 RNA: Update to v1.5.18 or later versions --------- End Update R Part 2 of 2 ---------. SIMATIC CP 1242-7C, SIMATIC CP 1243-1, SIMATIC CP 1243-7 LTE EU, SIMATIC CP 1243-7 LTE US, SIMATIC CP 1243-8 IRC: Update to v3.2 or later. SIMATIC CP 1542SP-1, SIMATIC CP 1542SP-1 IRC: Update to v2.1 or later versions. SIMATIC CP 1543-1: Update to v2.2 or later versions. SIMATIC CP 1543SP-1: Update to v2.1 or later versions. SIMATIC CP 1623: The updated firmware is contained in SIMATIC NET PC Software v14 Update 14 or later versions or SIMATIC NET PC Software v16 Update 5 or later versions. SIMATIC CP 1628: Update to v17.0 or later versions. SIMATIC ITC1500, SIMATIC ITC1500 PRO, SIMATIC ITC1900, SIMATIC ITC1900 PRO, SIMATIC ITC2200, SIMATIC ITC2200 PRO: Update to v3.1.1.0 or later versions. SIMATIC MV540 H, SIMATIC MV540 S, SIMATIC MV550 H, SIMATIC MV550 S, SIMATIC MV560 U, SIMATIC MV560 X: Update to v2.1 or later. SIMATIC Reader RF610R CMIIT, SIMATIC Reader RF610R ETSI, SIMATIC Reader RF610R FCC, SIMATIC Reader RF615R CMIIT, SIMATIC Reader RF615R ETSI, SIMATIC Reader RF615R FCC, SIMATIC Reader RF650R ARIB, SIMATIC Reader RF650R CMIIT, SIMATIC Reader RF650R ETSI, SIMATIC Reader RF650R FCC, SIMATIC Reader RF680R ARIB, SIMATIC Reader RF680R CMIIT, SIMATIC Reader RF680R ETSI, SIMATIC Reader RF680R FCC, SIMATIC Reader RF685R ARIB, SIMATIC Reader RF685R CMIIT, SIMATIC Reader RF685R ETSI, SIMATIC Reader RF685R FCC: Update to v4.0 or later versions. SIMATIC RF185C, SIMATIC RF186C, SIMATIC RF186CI, SIMATIC RF188C, SIMATIC RF188CI: Update to v1.3 or later versions. SIMATIC S7-1500 CPU 1518-4 PN/DP MFP: Update to v2.8.4. SINEMA Remote Connect Server: Update to v2.1. SINUMERIK 808D: Update to v4.92. The update can be obtained from a Siemens representative or via Siemens customer service. SINUMERIK 828D/840D sl: Update to v4.8 SP5. The update can be obtained from a Siemens representative or via Siemens customer service. SIPLUS ET 200SP CP 1543SP-1 ISEC, SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL: Update to v2.1 or later versions. SIPLUS NET CP 1543-1: Update to v2.2 or later versions. SIPLUS S7-1200 CP 1243-1, SIPLUS S7-1200 CP 1243-1 RAIL: Update to v3.2 or later versions. TIM 1531 IRC: Update to v2.1 or later versions Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:. Restrict network access to affected devices. Apply defense-in-depth. For SIMATIC Teleservice Adapters (IE Basic, IE Advanced): migrate to a successor product within the SCALANCE M-800 family. For details refer to the notice of discontinuation. As a general security measure, Siemens strongly recommends users protect network access to devices with As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens’ operational guidelines for industrial security and following recommendations in the product manuals. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. For more information, please see Siemens Security Advisory SSA-462066. CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:. Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov/ics. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the e ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 these vulnerabilities. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf2533865815b8**

Siemens has released updates for several affected products and recommends updating to the latest versions available. Siemens is preparing further updates and recommends countermeasures for products where updates are not, or not yet available. Please see Siemens SSA-772220 to determine if there is an update available.. 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, 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. For further inquiries on security vulnerabilities in Siemens products and solutions, please contact Siemens.. Additional Reference: SSA-772220 (PDF). Additional Reference: SSA-772220 (TXT). Additional Reference: SSA-772220 (CSAF). 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov/ics. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a499cf25338658158f**

Siemens has released updates for several affected products and is currently working on BIOS updates that include chipset microcode updates for further products.. SIMATIC Drive Controller family: Update BIOS to v05.00.01.00. The update can be obtained from a Siemens account manager. SIMATIC ET 200SP Open Controller CPU 1515SP PC2: Update BIOS to v0209\_0105 or later versions. SIMATIC Field PG M5: Update BIOS to v22.01.08. SIMATIC IPC127E: Update BIOS to v27.01.05. SIMATIC IPC427E (incl. SIPLUS variants): Update BIOS to v21.01.15. SIMATIC IPC477E: Update BIOS to v21.01.15. SIMATIC IPC477E Pro: Update BIOS to v21.01.15. SIMATIC IPC527G: Update BIOS to v1.4.0. SIMATIC IPC547G: Update BIOS to R1.30.0. SIMATIC IPC627E: Update BIOS to v25.02.08. SIMATIC IPC647E: Update BIOS to v25.02.08. SIMATIC IPC677E: Update BIOS to v25.02.08. SIMATIC IPC847E: Update BIOS to v25.02.08. SIMATIC ITP1000: Update BIOS to v23.01.08. SINUMERIK 828D HW PU.4: Update BIOS to v08.00.00.00. SINUMERIK software can be obtained from a Siemens account manager. SINUMERIK MC MCU 1720: Update BIOS to v05.00.00.00. SINUMERIK software can be obtained from a Siemens account manager. SINUMERIK ONE NCU 1740: Update BIOS to v04.00.00.00. SINUMERIK software can be obtained from a Siemens account manager. SINUMERIK ONE PPU 1740: Update BIOS to v06.00.00.00. SINUMERIK software can be obtained from a Siemens account manager Siemens has identified the following specific workarounds and mitigations users can apply to reduce risk:. Siemens recommends limiting the possibilities to run untrusted code.. Siemens recommends applying the defense-in-depth concept to reduce the probability for untrusted code to run on the system. As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens’ operational guidelines for industrial security and following recommendations in the product manuals.. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. For more information see Siemens Security Advisory SSA-678983. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. 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 on the ICS webpage on cisa.gov Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 these vulnerabilities. These vulnerabilities are not exploitable remotely. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf253386581566**

Siemens has released updates for several affected products and recommends users update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available. . SCALANCE X-200 switch family (incl. SIPLUS NET variants), All versions prior to v5.2.5: Update to v5.2.5 or later version. SCALANCE XB-200, All versions prior to v3.0: Update to v4.1. SCALANCE XC-200, All versions prior to v3.0: Update to v4.1. SCALANCE XP-200, All versions prior to v3.0: Update to v4.1. SCALANCE XF-200BA, All versions prior to v3.0: Update to v4.1. SCALANCE XR-300WG, All versions prior to v3.0: Update to v4.1. SCALANCE M-800, All versions prior to v4.3: Update to v6.1.2. SCALANCE S615, All versions prior to v4.3: Update to v6.1.2. Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200: Update to v4.5 Patch 01 . Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P: Update to v4.6 . PROFINET Driver for Controller: Update to v2.1 Patch 03. SCALANCE M-800 / S615: Update to v6.1.2. SCALANCE W700 IEEE 802.11n: Update to v6.4. SCALANCE X-200IRT switch family: Update to v5.4.2. SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG: Update to v4.1. SCALANCE XM-400 switch family: Update to v6.2.3. SCALANCE XR-500 switch family: Update to v6.2.3. SIMATIC CP 1616 and CP 1604: Update to v2.8.1. SIMATIC ET200MP IM155-5 PN HF: Update to v4.2.0. SIMATIC ET200MP IM155-5 PN ST: Update to v4.1.0. SIMATIC ET200SP IM155-6 PN HF: Update to v4.2.2. SIMATIC ET200SP IM155-6 PN ST: pdate to v4.1.0. SIMATIC RF600 family: Update to v3.2.1. SINAMICS DCP: Update to v1.3. SCALANCE X-300 switch family (incl. X408 and SIPLUS NET variants): Update to v4.1.4 or later --------- Begin Update H Part 1 of 1 ---------. SIMATIC NET CP 443-1 Advanced (incl. SIPLUS variants): Currently no fix planned. SIMATIC NET CP 443-1 (incl. SIPLUS variants): Currently no fix planned. SIMATIC NET CP 443-1 OPC UA: Currently no fix planned --------- End Update H Part 1 of 1 ---------. Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:. Block incoming DCE-RPC packets (port 34964/UDP) from untrusted networks . SCALANCE M-800 / S615 and RUGGEDCOM RM1224: Create a firewall rule that blocks the PROFINET Context Manager Port (34964/UDP) . Disable PROFINET in products, where PROFINET is optional and not used in your environment As a general security measure, Siemens strongly recommends users protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends users configure the environment according to Siemens’ operational guidelines for Industrial Security, and follow the recommendations in the product manuals.. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. For more information, please see Siemens security advisory: SSA-780073. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov/ics Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a499cf25338658153d**

Siemens recommends applying updates if available:. SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): Update to v2.1.7. SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): Update to v20.8. SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): Update to v2.8 . SIMATIC S7-1500 Software Controller: Update to v20.8 --------- Begin Update C Part 3 of 3 ---------. SIMATIC S7-1200 CPU family (incl. SIPLUS variants): Update to v4.5.2 or later --------- End Update C Part 3 of 3 ---------. Siemens has not identified any specific mitigations or workarounds and recommends following their general security recommendations. 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 the Siemens operational guidelines for Industrial Security and following the recommendations in the product manuals.. For additional information, please refer to Siemens Security Advisory SSA-593272. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov/ics Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a499cf253386581514**

Siemens has released updates for the following products:. SIMATIC HMI Unified Comfort Panels: Update to v17 or later. TIM 1531 IRC (incl. SIPLUS NET variants): Update to v2.2 or later --------- Begin Update B Part 2 of 2 ---------. SIMATIC NET CP 1545-1: Update to v1.1 or later --------- End Update B Part 2 of 2 ---------. SINUMERIK ONE MCP: Update to v2.0.1 or later. Please contact a Siemens representative for information on how to obtain the update. . SIMATIC NET CP 1543-1: Update to v3.0 or later Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:. Disable LLDP protocol support on Ethernet port. This will potentially disrupt the network visibility. 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 and following the recommendations in the product manuals.. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. Please see Siemens Security Advisory SSA-941426 for more information.. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov/ics Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 these vulnerabilities. This product is provided subject to this Notification and this Privacy & Use policy.

**CSAF: 62c3f0a499cf2533865814eb**

Siemens recommends the following workarounds and mitigations users can apply to reduce risk:. SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): Update to v6.0.10 or later version.. SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): Update to v2.0.0 or later version.. Limit access to Port 102/TCP to trusted users and systems only. 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 and to follow the recommendations in the product manuals.. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. For further inquiries on security vulnerabilities in Siemens products and solutions, please contact Siemens.. For additional information, please refer to Siemens Security Advisory SSA-446448 - PDF Version, SSA-446448 – TXT Version, or SSA-446448 – CSAF Version.. 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 they are not accessible from the Internet.. 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its 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 on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.

**CSAF: 62c3f0a499cf2533865814c2**

Siemens has released updates for several affected products and recommends updating to the latest versions available. Siemens is preparing further updates and recommends countermeasures for products where updates are not yet available or will not be developed. Please see Siemens SSA-712929 to determine if there is an update available.. As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens’ operational guidelines for industrial security and following recommendations in the product manuals.. Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage.. For more information see Siemens Security Advisory SSA-712929. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. 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 on the ICS webpage on cisa.gov/ics Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov/ics in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies. 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 and this Privacy & Use policy.