SEEPEX Security Updates						
Last Updated: 2 November 2026						SEEPEX. An Ingersoll Rand Business
No.	**Date of notification**	**Source**	**Bulletin**	**Impact**	**Affected SEEPEX product**	**Recommended action**
91	10/13/2026	Siemens	SSA-019113	Multiple vulnerabilities in the additional GNU/Linux subsystem may allow remote code execution, privilege escalation or denial of service. CVSS v3.1 10.0.	SIMATIC S7-1500 CPU family including related ET 200 CPUs and SIPLUS variants. Product and firmware level in installed base must be verified.	Update to Siemens fixed versions where available and apply mitigations. Verify affected S7-1500, ET 200 CPU and SIPLUS devices in service.
90	9/1/2026	Rockwell	SD1792 / CVE-2026-9637	Denial of Service through malformed CIP messages may trigger a Major Nonrecoverable Fault (MNRF), requiring a power cycle.	CompactLogix 5380, Compact GuardLogix 5380, ControlLogix 5580, GuardLogix 5580; firmware V33 and prior, V34.011-V34.014, V35.011-V35.013, V36.011-V36.012.	Update to firmware V37.011, V36.013, V35.014 or V34.015 as applicable.
89	9/8/2026	Schneider	SEVD-2026-251-04	Authentication bypass due to incorrect implementation of authentication algorithm. Unauthenticated connection may impact confidentiality, integrity and availability.	Modicon M580 (application level < 4.00); Modicon M580 Safety (application level < 4.20). Product and firmware level in installed base must be verified.	Update to Schneider remediation versions and application levels specified in advisory. Review controller firmware/application levels and restrict network access until updated.
88	8/11/2026	Schneider	CVE-2025-6625	Schneider Electric is aware of a vulnerability in its Modicon M340, BMXNOR0200H: Modicon M340 X80 Ethernet Communication Modules, BMXNGD0100: M580 Global Data module, BMXNOC0401: Modicon M340 X80 Ethernet Communication modules, BMXNOE0100: Modbus/TCP Ethernet Modicon M340 module, BMXNOE0110: Modbus/TCP Ethernet Modicon M340 FactoryCast module product(s). Failure to apply the fix provided below may risk Denial Of Service attack, which could result in the unavailability of the devices.	Modicon M340 BMXNOR0200H M580 Global Data module Modicon M340 X80 Ethernet Communication modules Modbus/TCP Ethernet Modicon M340 module	Update the Firmware to the newest Version
87	8/21/2026	Siemens	SSB-104599	The current geopolitical situation has created increased cybersecurity risks across all industrial sectors. This challenging environment also impacts the operational technology (OT) landscape, where we observe an intensification of threat activities. On 2025-06-30, CISA, FBI, DC3 and NSA published a joint advisory about an increased threat level for critical infrastructure and industrial control systems [0]. On 2026-04-07, a new advisory was published, which now additionally flags Siemens S7 PLCs as potentially targeted [1]. Following this, on 2026-07-28, the existing advisory was updated to additionally flag the Siemens S7-1200 PLC as a specifically named target in the ongoing threat campaign [1]. On 2026-08-19, a new advisory was published specifically focusing on an potential active threat against the Siemens S7 series programmable logic controllers (PLCs) [10]. Given these developments, Siemens strongly recommends that customers review and implement the necessary measures to protect their infrastructure. Siemens provides assistance via its Industrial Cybersecurity offerings [11]. To learn more, please contact your Siemens Sales representative.	Siemens S7-1200 Gen1 Siemens S7-1200 Gen2 Siemens S7-1500	SECURITY MEASURES Keep the devices and systems updated to the latest version to limit the attack vectors that might exploit known vulnerabilities. Disconnect or remove any devices from networks with inadequate security level (internet, unmaintained internal networks, inadequate physically secured environments etc.) or install additional protection measures (e.g. firewalls). Use strong, unique passwords; do not use default password; use long enough and complex passwords. Follow the Siemens Operational Guidelines for Industrial Security [2]. Refer to device specific user documentation to stay informed and avoid potential misconfigurations [5][6][7][8][9].
86	8/11/2026		SSA282044	The installers used to install several Siemens products are affected by a DLL hijacking vulnerability. This could allow an attacker to execute arbitrary code when a legitimate user installs an application that uses the affected installer component. This vulnerability poses a risk only during setup and installation phase of the affected applications downloaded e.g. via OSD (Online Software Delivery). Siemens has released new versions for several affected products and recommends using the latest versions during setup and installation. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available	SIMATIC S7-PLCSIM SIMATIC WinCC	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
85	8/11/2026	Siemens	SSA-392349	Multiple industrial devices contain a vulnerability that could allow an attacker to cause a denial of service condition. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	Scalance X-200 family Siemens S7-1200 family Siemens S7-1500 family	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
84	14/07/2026	Siemens	SSA-828211	SIMATIC S7-PLCSIM Advanced contains a vulnerability that could allow an attacker to cause a denial of service condition.	SIMATIC S7-PLCSIM Advanced All versions	Currently no fix is available
83	14/07/2026	Siemens	SSA-688146	SIMATIC S7 PLCs contain multiple vulnerabilities in the web server that could allow an attacker to perform cross-site scripting attacks.	SIMATIC S7-1500 CPU family	Update to V2.9.9 or later version
82	14/07/2026	Rockwell Automation	CVE-2026-10573	A denial-of-service security issue exists in 1734 POINT I/O™ module. The security issue stems from improper handling of crafted CIP messages, which can cause the module to enter a faulted state. A restart is required to recover.	1734 POINT I/O™ Firmware Version 3.023 or later	Users are recommended to migrate to 5034-OB8

81	14/07/2026	Rockwell Automation	CVE-2025-11698	A denial-of-service issue exists in 5380/5480/5580 controllers boot firmware lower than version 1.072. This vulnerability could potentially allow a malicious user to write invalid file data to the controller, causing the device to enter a major non-recoverable fault (MNRF).	CompactLogix® 5380 Recovery Image Boot firmware versions before 1.072	Boot firmware 1.072 or greater If using V36.013, V37.011 or later, already has corrected boot firmware is installed
80	14/07/2026	Rockwell Automation	CVE-2025-12012	A denial-of-service issue exists in 5380/5480/5580 controllers. This vulnerability could potentially allow a malicious user to write invalid file data to the controller, causing the device to enter a major non-recoverable fault (MNRF).	CompactLogix® 5380 V35.011 or later	Corrected in Firmware Version 36.011 and later
79	14/07/2026	Rockwell Automation	SD1783	A path traversal security issue exists within Studio 5000 Logix Designer® due to improper limitation of file paths within ACD project files. The software does not sanitize or validate file names embedded in the ACD file structure during the project opening procedure, allowing path traversal sequences to escape the intended extraction directory. If exploited, an attacker could craft a malicious ACD project file that results in arbitrary files being written to attacker-controlled locations on the file system, potentially leading to code execution. A remote code execution security issue exists within Studio 5000 Logix Designer® due to incorrect authorization on a configuration file. This can allow any authenticated user to modify the paths of external tools configured within the application. If exploited, an attacker could alter the configuration to point to a malicious executable, resulting in arbitrary code execution when any user interacts with the external tools functionality. A code execution security issue exists within Studio 5000 Logix Designer® due to an unquoted search path in the External Tools configuration. The executable paths specified in the external tools configuration file are not properly quoted, and because these paths contain spaces, the operating system may resolve them to unintended executables placed earlier in the search order. If exploited, an attacker could plant a malicious executable in a location within the search path, resulting in arbitrary code execution with the same permissions of the user running the application.	Studio 5000 Logix Designer 36.00 or later	Corrected in Firmware Version 37.00 or higher
78	14/07/2026	Rockwell Automation	CVE-2026-9636	A security issue exists within CompactLogix® 5380, ControlLogix® 5580, and EN4TR communication modules related to CIP Security certificate revocation handling. The security issue stems from the controller failing to properly reject certificates signed by an intermediate certificate that has been revoked via a Certificate Revocation List (CRL). This could allow a network-based attacker to establish a connection using a certificate that should be untrusted, potentially bypassing CIP Security protections.	CompactLogix® 5380 V2 or later	Corrected in Firmware Version 38.011
77	6/6/2026	Siemens	SSA-674753	Siemens ET 200 devices contain a denial-of-service vulnerability that could be triggered by sending a valid S7 protocol Disconnect Request (COTP DR TPDU), causing the device to become unresponsive and require a power cycle to recover. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	Industrial devices ET200	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
76	5/12/2026	Siemens	SSA-392349	Multiple industrial devices contain a vulnerability that could allow an attacker to cause a denial of service condition. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	Industrial devices	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

75	4/14/2026	Siemens	SSA-599968	A vulnerability in affected devices could allow an attacker to perform a denial ofservice attack if a large amount of Profinet Discovery and Configuration Protocol (DCP) reset packets is sent to the affected devices. 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.	PROFINET Devices	Siemens has identified the following specific mitigations that customers can apply to reduce the risk: Disable Profinet in products, where Profinet is optional and not used in your environment Block incoming Profinet Discovery and Configuration Protocol (DCP) packets (Ethertype 0x8892, Frame-ID: 0xfefe) from untrusted networks Product-specific remediations or mitigations can be found in the section Known Affected Products. 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
74	4/14/2026	Siemens	SSA-710008	SCALANCE devices contain multiple vulnerabilities in MSPS based product lines that could allow authenticated remote attackers to execute custom code or create a XSS situation, as well as unauthenticated remote attackers to create a denial of service condition. Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.	SCALANCE Products	Siemens has identified the following specific mitigations that customers can apply to reduce the risk: Apply the principle of least privileges for accounts configured on the affected devices Restrict network access in affected system(s) to ports 80/TCP and 443/TCP to trusted IP addresses and personal only Product-specific remediations or mitigations can be found in the section Known Affected Products. 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
73	3/10/2026	Rockwell Automation	CVE-2021-22681	Researchers found that Rockwell Automation Studio 5000 Logix Designer® software may allow a cryptographic key to be discovered. This internal licensing key is used by Rockwell Automation design software to communicate with Logix controllers. If successfully exploited, this vulnerability could allow a non-Rockwell Automation application to connect with Logix controllers. To leverage this vulnerability, an unauthorized user would require network access to the controller.	CompactLogix® 5380 v28 or later.	Install the 1783-CSP CIP Security Proxy to provide secure connection between the engineering workstation and the controller. For more information, please see the 1783-CSP CIP Proxy User Manual (link).
72	3/19/2026	Siemens	SSA-452276	SIMATIC S7-1500 devices contain a vulnerability that could allow an attacker to inject code by tricking a legitimate user into importing a specially crafted trace file in the web interface.	SIMATIC S7-1500 CPU family	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
71	2/18/2026	B&R	SA25P007	An update is available that replaces an outdated third-party component affected by publicly disclosed vulnerabilities in the product versions listed above. Although no successful exploitation was observed during testing of the affected B&R products, the identified vulnerabilities could present potential attack vectors that might enable unauthorized access, data exposure, or remote code execution	Automation Studio < 6.5	The problem is corrected in the following product versions: B&R Automation Studio 6.5 B&R recommends that customers apply the update at earliest convenience. The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual.
70	1/19/2026	B&R	SA25P004	A vulnerability exists in the ANSL and OPC-UA clients included in the product versions listed above. An attacker could exploit a vulnerability by spoofing a trusted entity when Automation Studio is connecting to an ANSL or OPC-UA server. The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)1 for both v3.12 and v4.03 . The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list4	Automation Studio < 6.5	The problem is corrected in the following product versions: B&R Automation Studio version 6.5 B&R recommends that customers apply the update at earliest convenience. The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual

69	1/13/2026	Siemens	SSA-674753	Siemens ET 200SP contains a denial-of-service vulnerability that could be triggered by sending a valid S7 protocol Disconnect Request (COTP DR TPDU), causing the device to become unresponsive and require a power cycle to recover. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC ET 200SP SIMATIC PN/PN Coupler	Siemens has identified the following specific mitigations that customers can apply to reduce the risk: Restrict access to the network where S7 communication messages are exchanged. Filter the port 102 of the devices to only accepted connections to/from the IP addresses of machines that are trusted e.g. with an external firewall.
68	12/9/2025	Siemens	SSA-915282	Multiple Industrial products are affected by a vulnerability in the Interniche IP-Stack. The affected products do not properly enforce TCP sequence number validation in specific scenarios but accept values within a broad range. This could allow an unauthenticated remote attacker e.g. to interfere with connection setup, potentially leading to a denial of service. The attack succeeds only if an attacker can inject IP packets with spoofed addresses at precisely timed moments, and it affects only TCP-based services.	SIMATIC ET 200SP SIMATIC PN/PN Coupler SIMATIC S7-1200 CPU V4 family SIMATIC S7-1500 family	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
67	12/9/2025	Siemens	SSA-800126	Affected products do not properly sanitize user-controllable input when parsing files. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	SIMATIC S7-PLCSIM Totally Integrated Automation Portal (TIA Portal)	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available. Siemens has released products based on the Totally Integrated Automation Portal (TIA Portal) V20 which are not affected by CVE-2024-49849. See the chapter "Additional Information" below for more details.
66	12/9/2025	Siemens	SSA-693808	Affected products do not properly restrict access permissions to a local Windows Named Pipe and do not properly sanitize user-controllable input sent to that Named Pipe. This could allow a local authenticated attacker to cause a type confusion and execute arbitrary code within the affected application and its privileges.	SIMATIC S7-PLCSIM V17 Totally Integrated Automation Portal (TIA Portal)	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
65	12/9/2025	Siemens	SSA-493396	Affected products do not properly sanitize user-controllable input when parsing project files. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	SIMATIC S7-PLCSIM V17 Totally Integrated Automation Portal (TIA Portal)	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
64	12/9/2025	Siemens	SSA-392859	Affected products contain a local arbitrary code execution vulnerability that could allow an attacker to perform actions against the operation system of that environment.	SIMATIC S7-PLCSIM Totally Integrated Automation Portal (TIA Portal)	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available. Siemens has released products based on the Totally Integrated Automation Portal (TIA Portal) V20 which are not affected by CVE-2024-52051. See the chapter "Additional Information" below for more details.
63	12/8/2025	Siemens	SSA-282044	The installers used to install several Siemens products are affected by a DLL hijacking vulnerability. This could allow an attacker to execute arbitrary code when a legitimate user installs an application that uses the affected installer component. This vulnerability poses a risk only during setup and installation phase of the affected applications downloaded e.g. via OSD (Online Software Delivery).	Automation License Manager SIMATIC S7-PLCSIM SIMATIC WinCC TIA Administrator Totally Integrated Automation Portal (TIA Portal)	Siemens has released products based on the Totally Integrated Automation Portal (TIA Portal) V20 which are not affected by CVE-2024-52051. See the chapter "Additional Information" below for more details.
62	11/11/2025	Siemens	SSA-711309 V2.5	The OPC UA implementations (ANSI C and C++) as used in several SIMATIC products contain a denial of service vulnerability that could allow an unauthenticated remote attacker to create a denial of service condition by sending a specially crafted certificate. 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.	SIMATIC WinCC	WORKAROUNDS AND MITIGATIONS Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Disable the OPC UA feature, if not used Product-specific remediations or mitigations can be found in the section Known Affected Products. Please follow the General Security Recommendations.

61	10/14/2025	Rockwell Automation	SD 1757	The 1715 EtherNet/IP Communications Module is a fault-tolerant adapter designed for high-availability applications, enabling redundant I/O communication over EtherNet/IP.	1715-AENTR EtherNet/IP Adapter	Remedial measures and workarounds Customers using the affected software, who are not able to upgrade to one of the corrected versions, should use our security best practices.
60	10/14/2025	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successful attack, the legitimate user must actively click on an attacker-crafted link. 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.	SIMATIC S7-1500 SIMATIC S7-1200	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: • Do not click on links from unknown sources. Product-specific remediations or mitigations can be found in the section Known Affected Products. Please follow the General Security Recommendations.
59	10/14/2025	Schneider Electrics	CVE-2024-6528	Schneider Electric is aware of a vulnerability in its Modicon Controllers M241 / M251, M258 / LMC058, and M262 products. The Modicon Controllers M241 / M251 / M258 / M262 and Modicon Motion Controller LMC058 are Programmable Logic Controllers for performance-demanding applications. Failure to apply the remediation provided below may risk a Cross-site Scripting or an open redirect attack which could result in an account takeover scenario or the execution of code in the user browser. October 2025 Update: A remediation is now available for Modicon Controllers M258 / LMC058.	Modicon M241 /M251 - Alle Versionen vor V5.2.11.24 Modicon M258 /LMC508 - Alle Versionen vor V5.0.4.19 Modicon M262 - Alle Versionen vor V5.2.8.26	We strongly recommend the following industry cybersecurity best practices. • Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network. • Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks. • Place all controllers in locked cabinets and never leave them in the “Program” mode. • Never connect programming software to any network other than the network intended for that device. • Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks. • Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation. • Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet. • When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices. For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

58	9/9/2025	Siemens	SSA-503939	Multiple vulnerabilities have been identified in the BIOS of the SIMATIC S7-1500 TM MFP. Siemens is preparing fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1500 TM MFP - BIOS	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Only build and run applications from trusted sources Please follow the General Security Recommendations.
57	9/9/2025	Siemens	SSA-691715	A vulnerability was identified in OPC Foundation Local Discovery Server which also affects Siemens products that could allow an attacker to escalate privileges under certain circumstances. 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.	OpenPCS 7 V9.1 SIMATIC NET PC Software SIMATIC WinCC SIMATIC WinCC Runtime Professional SIMATIC WinCC Unified PC Runtime V18	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Update the underlying OPC Foundation Unified Architecture Local Discovery Server (UA-LDS) to V1.04.405 or later if possible Product-specific remediations or mitigations can be found in the section Known Affected Products. Please follow the General Security Recommendations.
56	8/14/2025	Rockwell Automation	SD 1734	DETAILS ABOUT THE SECURITY VULNERABILITY Rockwell Automation used the latest version of the CVSS scoring system to evaluate the following security vulnerabilities. CVE-2025-7971 IMPACT Due to insecure processing of environment variables, there is a security vulnerability in Studio 5000 Logix Designer. If the specified path does not contain a valid file, Logix Designer crashes. However, it is possible to execute malicious code without causing a crash. CVSS 3.1 Base Score: 7.5 CVSS 3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:C/C:H/I:H/A:H CVSS 4.0 Base Score: 7.3 CVSS 4.0 vector: CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N CWE: CWE-20: Improper Input Validation Known Exploited Vulnerabilities (KEV) database: No	Studio 5000 Logix Designer 36.00.02	Remedial measures and workarounds Users should update to the corrected version if possible. If users who use the affected software cannot upgrade the version, best security practices should be applied.
55	8/14/2025	Rockwell Automation	SD 1732	Rockwell Automation has used the latest version of the CVSS scoring system to assess the following vulnerabilities. CVE-2025-7353 IMPACT A security issue exists due to the web-based debugger agent enabled on released devices. If a specific IP address is used to connect to the WDB agent, attackers can remotely create memory dumps, modify memory, and control execution flow. CVSS 3.1 Base Score: 9.8 CVSS 3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS 4.0 Base Score: 9.3 CVSS 4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N CWE: CWE-1188: Initializing a resource with an insecure default setting Known Exploited Vulnerabilities Database (KEV): No	1756-EN2T/D,1756-EN2F/C, 1756-EN2TR/C, 1756-EN3TR/B, 1756-EN2TP/A Version 11.004 or below	Remedial measures and workarounds Users should update to the corrected version if possible. If users who use the affected software cannot upgrade the version, best security practices should be applied.

54	8/12/2025	Schneider Electrics	CVE-2025-6625	Schneider Electric has identified a security vulnerability in its Modicon M340, BMXNOR0200H: Modicon M340 X80 Ethernet communication modules, BMXNGD0100: M580 Global Data module, BMXNOC0401: Modicon M340 X80 Ethernet communication modules, BMXNOE0100: Modbus/TCP Ethernet Modicon M340 module, BMXNOE0110: Modbus/TCP Ethernet Modicon M340 FactoryCast module products. If the fix below is not applied, there is a risk of a denial-of-service attack that could result in the devices becoming unavailable	Modicon M340 All versions BMXNOE0100: Modbus/TCP Ethernet Modicon M340 module Versions prior to SV3.60 BMXNOE0110: Modbus/TCP Ethernet Modicon M340 FactoryCast module Versions prior to SV6.80	We strongly recommend the following best practices for industrial cybersecurity. • Place control and security system networks and remote devices behind firewalls and isolate them from the corporate network. • Install physical controls to prevent unauthorized personnel from accessing your industrial control and security systems, components, peripherals, and networks. Security Advisory from Schneider Electric August 12, 2025 Document Reference Number – SEVD-2025-224-05 Page 4 of 5 Public / TLP: Released • Keep all controllers in locked cabinets and never leave them in “program” mode. • Never connect programming software to any network other than the network intended for that device. • Scan all methods of mobile data exchange with the isolated network, such as CDs, USB sticks, etc., before use in the terminals or at a node connected to these networks. • Never allow mobile devices that have been connected to a network other than the intended network to connect to the security or control networks without proper cleaning. • Minimize network exposure for all control system devices and systems and ensure that they are not accessible via the Internet. • If remote access is required, use secure methods such as Virtual Private Net Please note that VPNs may have vulnerabilities and should be updated to the latest available version. Also note that VPNs are only as secure as the devices connected to them. For more information, see Schneider Electric's recommended cybersecurity measures.
53	8/12/2025	Schneider Electrics	CVE-2024-5056	Schneider Electric is aware of a security vulnerability in its Modicon M340, BMXNOE0100, and BMXNOE0110 products. The Modicon M340 is a programmable logic controller; BMXNOE0100 and BMXNOE0110 are network modules used with the Modicon M340. If the workarounds listed below are not implemented, users may not be able to update the device firmware and the web server may not function properly. The operation of BMXNOE and Modicon M340 is not affected by this security vulnerability. August update: Workarounds are available for BMXNOE0100 (Modbus/TCP Ethernet Modicon M340 module) and BMXNOE0110 (Modbus/TCP Ethernet Modicon M340 FactoryCast module).	Modicon M340 All versions BMXNOR0200H: Ethernet / Serial RTU Module All versions BMXNGD0100: M580 Global Data module All versions BMXNOC0401: Modicon M340 X80 Ethernet Communication modules All versions BMXNOE0100: Modbus/TCP Ethernet Modicon M340 module Versions prior to 3.60 BMXNOE0110: Modbus/TCP Ethernet Modicon M340 FactoryCast module Versions prior to 6.80	General security recommendations We strongly recommend the following best practices for industrial cybersecurity. • Place networks for control and safety systems and remote devices behind firewalls and isolate them from the corporate network. • Install physical controls to prevent unauthorized personnel from accessing your industrial control and security systems, components, peripherals, and networks. • Keep all controllers in locked cabinets and never leave them in “program” mode. • Never connect programming software to any network other than the one intended for that device. • Scan all methods of mobile data exchange with the isolated network, such as CDs, USB sticks, etc., before using them in terminals or other nodes connected to these networks. • Never allow mobile devices that have been connected to a network other than the intended network to connect to the security or control networks without proper cleaning. Security Advisory from Schneider Electric June 24, 2011 (August 25, 2012) Document Reference Number – SEVD-2024-163-01(v2.0.0) Page 4 of 5 Public / TLP: Approved • Minimize network exposure for all control system devices and systems and ensure that they are not accessible via the Internet. • If remote access is necessary, use secure methods such as virtual private networks (VPNs). Note that VPNs can have vulnerabilities and should be updated to the latest available version. Also note that VPNs are only as secure as the connected devices.
52	8/18/2025	Siemens	SSA-711309	The OPC UA implementations (ANSI C and C++) used in several SIMATIC products contain a denial-of-service vulnerability that could allow an unauthenticated attacker to create a denial-of-service condition by sending a specially crafted certificate. Siemens has released new versions for several affected products and recommends updating to the latest versions. Siemens recommends specific countermeasures for products for which no fixes are available or are not yet available.	SIMATIC WinCC Unified OPC UA Server SIMATIC WinCC OPC UA Client SIMATIC WinCC Runtime Professional SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants)	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Disable the OPC UA function if it is not in use. Product-specific mitigations or workarounds can be found in the Affected Products and Solutions section. Please note the general security recommendations.
51	8/12/2025	Siemens	SSA-460466	A vulnerability in TIA Project Server and TIA Portal could allow an attacker to cause a denial-of-service condition. Siemens has released new versions for several affected products and recommends updating to the latest versions. Siemens is preparing further corrective versions and recommends countermeasures for products for which no corrections are available or are not yet available.	Totally Integrated Automation Portal (TIA Portal) V18 & V20	Product-specific remedies or protective measures can be found in the section “Known affected products.” Please follow the general security recommendations.

50	8/12/2025	Siemens	SSA-353002	The SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family is affected by several security vulnerabilities. CVE-2023-44318 and CVE-2023-44321 were previously published as part of SSA-699386.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Familie.	As a general security measure, Siemens strongly recommends protecting network access to the devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment in accordance with the Siemens operating guidelines for industrial security (download: https://www.siemens.com/cert/operational-guidelines-industrial-security) and to follow the recommendations in the product manuals. For more information on industrial security from Siemens, visit: https://www.siemens.com/industrialsecurity
49	8/12/2025	Siemens	SSA-800126	Affected products do not properly sanitize user-controllable input when parsing files. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. Siemens has released new versions for several affected products and recommends updating to the latest versions. Siemens is preparing further corrective versions and recommends specific countermeasures for products for which no corrections are available or are not yet available. Siemens has released products based on the Totally Integrated Automation Portal (TIA Portal) V20 that are not affected by CVE-2024-49849. For more information, see the “Additional Information” section below.	SIMATIC S7-PLCSIM V16 Totally Integrated Automation Portal V16, V17, V18 (TIA Portal)	Siemens has identified the following specific workarounds and remedies that customers can apply to mitigate the risk: CVE-2024-49849: Avoid opening untrusted files from unknown sources in affected products.
41	6/10/2025	Siemens	SSA-858251	The products listed below contain two authentication bypass vulnerabilities that could allow an attacker to gain access to the data managed by the server. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	OPC UA	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
40	13.05.2025	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successful attack, the legitimate user must actively click on an attacker-crafted link. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1200 / S7-1500 CPUSiemens can be found at: https://www.siemens.com/industrialsecurit	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: • Do not click on links from unknown sources. 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

39	5/13/2025	Siemens	SSA-054046	Several SIMATIC S7-1500 CPU versions are affected by an authentication bypass vulnerability that could allow an unauthenticated remote attacker to gain knowledge about actual and configured maximum cycle times and communication load of the CPU. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1500 CPU SIMATIC ET 200SP	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
38	4/8/2025	Schneider Electric Security Notification	CVE-2024-8936	Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 products. Modicon PAC control and monitor industrial operations. Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controller, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller. April 2025 Update: A remediation is now available for Modicon Momentum Unity M1E ProcessorVersion prior to SV3.65	Modicon M340 CPU (part numbers BMXP34*)	Version SV3.65 of Modicon M340 firmware includes a fix for these vulnerabilities
37	4/8/2025	Schneider Electric Security Notification	CVE-2020-28895	Schneider Electric is aware of multiple memory allocation vulnerabilities dubbed 'BadAlloc', disclosed by Microsoft on April 29, 2021. The impact of a successful exploitation of the vulnerabilities may result in denial of service, or remote code execution, depending on the context. April 2025 Update: A remediation is available for BMECRA31210, BMXCRA31200, BMXCRA31210 (Page 13) and mitigations for this product have been updated.	Modicon M340 CPU (BMXP34*) v3.40 and prior	Version 3.50 of Modicon M340 includes a fix for these vulnerabilities
36	4/8/2025	Siemens Security Advisory by Siemens ProductCERT	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successful attack, the legitimate user must actively click on an attacker-crafted link.	SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.7	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
35	4/8/2025	Siemens Security Advisory by Siemens ProductCERT	SSA-725549	A vulnerability exists in affected products that could allow remote attackers to affect the availability of the devices under certain conditions. The integrated ICMP services in the underlying TCP/IP stack is vulnerable to a denial of service attack through specially crafted ICMP packets. A successful attack will impact the availability of ICMP services on affected products for a limited time before it restores itself after the attack ceases. Other communication services are not affected by this vulnerability.	SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0) All versions SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.4	Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.
34	4/8/2025	Siemens Security Advisory by Siemens ProductCERT	SSA-195895	The webserver of several SIMATIC products is affected by a user enumeration vulnerability that could allow an unauthenticated remote attacker to identify valid usernames.	SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.7	Siemens has released new versions for the affected products and recommends to update to the latest versions.
33	3/11/2025	Siemens	SSA-858251	The products listed below contain two authentication bypass vulnerabilities that could allow an attacker to gain access to the data managed by the server. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	Totally Integrated Automation Por-tal (TIA Portal) V18, V19	Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.
32	3/11/2025	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerabilty that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successful attack, the legitimate user must actively click on an at-tacker-crafted link. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific counter-measures for products where fixes are not, or not yet available.	S7-1200 CPU / S7-1500 CPU	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
31	3/11/2025	Siemens	SSA-054046	Several SIMATIC S7-1500 CPU versions are affected by an authentication bypass vulnerability that could allow an unauthenticated remote attacker to gain knowledge about actual and configured maximum cycle times and communication load of the CPU. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.		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

30	2/11/2025	Schneider	Vulnerabilities Details	The Modicon Programmable Automation controllers are used for complex networked communication, display and control applications Failure to apply the mitigations or remediations provided below may risk execution of unsolicited command on the PLC which could result in a loss of availability of the controller February 2025 Update: Correction of vulnerabilities impacting Quantum Safety processor	Modicon Controller M340, M580	Update Software and Firmware and Rebuild the Projects
29	2/11/2025	Siemens	SSA-195895	The webserver of several SIMATIC products is affected by a user enumeration vulnerability that could allow an unauthenticated remote attacker to identify valid usernames. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1200 CPU family V4 (incl. SIPLUS variants) SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) SIMATIC S7-PLCSIM Advanced All versions >= V6.0 < V7.0	Update to V4.7 or later version Update to V3.1.2 or later version.Disable HTTP (port 80/tcp) and provide web service access through HTTPS (port 443/tcp) only; the vulnerability is considered as only exploitable via HTTP Update to V7.0 or later version Disable HTTP (port 80/tcp) and provide web service access through HTTPS (port 443/tcp) only; the vulnerability is considered as only exploitable via HTTP
28	2/11/2025	Siemens	SSA-224824	SIMATIC S7-1200 CPU family before V4.7 is affected by two denial of service vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions.SIMATIC S7-1200 CPU family before V4.7 is affected by two denial of service vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions.	SIMATIC S7-1200 CPU family V4 (incl. SIPLUS variants)	Update to V4.7 or later version
27	2/11/2025	Siemens	SSA-342348	Affected products do not correctly invalidate user sessions upon user logout. This could allow a remote unauthenticated attacker, who has obtained the session token by other means, to re-use a legitimate user's session even after logout. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where fixes are not, or not yet available.	TIA Administrator All versions < V3.0.4 Totally Integrated Automation Portal (TIA Portal)	Update to V3.0.4 or later version Update to V19 Update 1 or later version
26	2/11/2025	Siemens	SSA-349422	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.	SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants)	Update to V4.2.0 or later version
25	2/11/2025	Siemens	SSA-712929	A vulnerability in the openSSL component (CVE-2022-0778, [0]) could allow an attacker to create a denial of service condition by providing specially crafted elliptic curve certificates to products that use a vulnerable version of openSSL. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	SCALANCE XC208 SIMATIC CP 1243-1 SIMATIC ET 200SP communications modules (CP 1542SP-1, CP 1542SP-1 IRC and CP 1543SP-1, incl. SIPLUS variants) SIMATIC S7-1200 CPU family (incl. SIPLUS variants) SIMATIC S7-1500 CPU 1513R-1 PN SIMATIC S7-PLCSIM Advanced SIMATIC WinCC V7/V8 Totally Integrated Automation Portal (TIA Portal) V16	Update to V4.4 or later version Update to V3.4.29 or later version Update to V2.2.28 or later version Update to V4.6.0 or later version Update to V2.9.7 or later version Update to V5.0 or later version Update to V7.5 SP2 Update 16 or later version Currently no fix is planned
24	1/14/2025	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successful attack, the legitimate user must actively click on an attacker-crafted link. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) SIMATIC S7-1500 Software Controller	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Do not click on links from unknown sources. Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

23	1/14/2025	Siemens	SSA-730482	A vulnerability in the login dialog box of SIMATIC WinCC could allow a local attacker to cause a denial of service condition in the runtime of the SCADA system. Siemens has released new versions for the affected products and recommends to update to the latest versions.	SIMATIC WinCC Runtime Professional SIMATIC PCS 7	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Activate SIMATIC Logon in the User Administrator of the SIMATIC PCS 7 Operator Stations Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.
22	1/14/2025	Siemens	SSA-711309	The OPC UA implementations (ANSI C and C++) as used in several SIMATIC products contain a denial of service vulnerability that could allow an unauthenticated remote attacker to create a denial of service condition by sending a specially crafted certificate. 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.	SIMATIC WinCC Unified OPC UA Server SIMATIC WinCC OPC UA Client SIMATIC WinCC Runtime Professional SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants)	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Disable the OPC UA feature, if not used Product-specific remediations or mitigations can be found in the section Affected Products and Solution.
21	1/14/2025	Siemens	SSA-413565	Multiple SCALANCE devices are affected by several vulnerabilities that could allow an attacker to inject code, retrieve data as debug information as well as user CLI passwords or set the CLI to an irresponsive state. Siemens has released updates for the affected products and recommends to update to the latest versions.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family	Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.
20	12/10/2024	Siemens	SSA-711309	The OPC UA implementations (ANSI C and C++) as used in several SIMATIC products contain a denial of service vulnerability that could allow an unauthenticated remote attacer to create a denial of service condition by sending a specially crafted certificate. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) SIMATIC Win CC OPC UA Client SIMATIC WinCC Runtime Professional SIMATIC WinCC Unified OPC UA Server	Update to V2.0.0.1 or later version See further recommendations from section Workarounds and Mitigations
19	12/10/2024	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL. For a successfull attack, the legitimate user must actively click on an attacker-crafted link. Siemens has released new versions for several affected products and recommends to update to the latest versions. Simens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-1500 Software Controller	Currently no fix available See further recommendations from section Workarounds and Mitigations
18	11/12/2024	Siemens	SSA-871035	Affected products do not preoperly sanitize user-controllable input when parsing files. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	SIMATIC S7-PLCSIM V16 Totally Integrated Automation Portal V16, V17, V18 (TIA Portal)	No solution available yet. Please see here for further information.
17	10/8/2024	Siemens	SSA-054046	Several SIMATIC S7-1500 CPU versions are affected by an authentification bypass vulnerability that could allow an unauthenticated remote attacker to gain knowledge about actual and configured maximum cycle times and communication load of the CPU. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.	All S7-1500 CPUs	Product-specific remediations or mitigations can be found in the section Affected Products and Solutions. Please follow the General Security Recommendations
16	10/8/2024	Siemens	SSA-876787	Several SIMATIC S7-1500 and S7-1200 CPU versions are affected by an open redirect vulnerability that could allow an attacker to make the web werver of affected devices redirect a legitimate user to an attacker-chosen URL. Fo a successful attack, the legitimate user needs to actively click on an attacker-crafted link. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.	Simatic S7-1200 CPU Family Simatic S7-1500 CPU Family	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk Do not click on links from unknown sources. Product-specific remeditations or mitigations can be found in the section Affected Products and Solutions. Please follow the General Security Recommendations.
15	8/13/2024	Rockwell Automation	SD 1685	A denial-of-service vulnerability exists in the affected product. This vulnerability occurs when a malformed PCCC message is received, causing a failure in the controller.	ControlLogix/GuardLogix 5580 and Compact-Logix/Compact GuardLogix® 5380 Controller	Update to latest firmware revision. Restrict communication to CIP objects 103 (0x67)

14	7/9/2024	Siemens	SSA-779936	Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	Totally Integrated Automation Portal (TIA Portal) before V19	Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk: Avoid opening untrusted files from unknown sources in affected products
13	7/9/2024	Siemens	SSA-473245	A vulnarability in affected devices could allow an attacker to perform a denial of service attack if a large amount of specially crafted UDP packets are sent to the device. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific counter measures for products where fixes are not, or not yet available.	Simatic S7-1200 CPU Family, Simatic S7-1500 Family, ET200SP	Siemens has identifid the following specific workarounds and mitigations that customers cann apply to reduce the risk: Restrict network access to affected devices
12	6/11/2024	Siemens	SSA-319319	TIA Administrator creates temporary download files in a directory with insecure permissions. This could allow any authenticated attacker on Windows to disrupt the update process.	TIA-Administrator <3.2	Siemens has released a new version for TIA Administrator and recommends to update to the latest version. Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk. Remove write permissions for non-administrative users on files and folders located under the installation path
11	6/11/2024	Siemens	SSA-353002	The SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG group is affected by multiple vulnerabilities. CVE-2023-44318 and CVE-2023-44321 were previously published as part of SSA-699386.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG group.	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
10	6/11/2024	Siemens	SSA-711309	Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Products	All SEEPEX control featuring the following SIEMENS Software: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP	Currently no fix available/ Update to latest version
9	5/21/2024	Rockwell Automation	SD1672	IMPORTANT NOTICE: Rockwell Automation reiterates the instruction to its customers to disconnect devices from the Internet to protect against cyber threats Due to heightened geopolitical tensions and hostile cyber activity around the world, Rockwell Automation urges all customers to IMMEDIATELY check if their devices are connected to the public Internet and, if so, to urgently remove that connection for devices that are not specifically designed for a public Internet connection.	All SEEPEX controls with Rockwell Automation Hardware	Due to heightened geopolitical tensions and adversarial cyber activity globally, Rockwell Automation is issuing this notice urging all customers to take IMMEDIATE action to assess whether they have devices facing the public internet and, if so, urgently remove that connectivity for devices not specifically designed for public internet connectivity.
8	5/14/2024	Siemens	SSA-592380	A vulnerability has been discovered in the SIMATIC S7-1500 CPU family and related products that could allow an attacker to trigger a denial of service condition. In order to exploit the vulnerability, an attacker must have access to the affected devices on port 102/tcp.	All SEEPEX controls with the following SIEMENS hardware: SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0)	No solution is currently planned
7	2/13/2024	Siemens	SSA-711309	Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Products	All SEEPEX controls featuring the following SIEMENS Software: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP	Currently no fix available / Update to latest version
6	12/12/2023	Siemens	SSA-887801	Information disclosure to LOCAL attacker to the access level password of the SIMATIC S7-1200 and S7-1500 CPUs	All SEEPEX controls featuring the following SIEMENS hardware: SIMATIC S7-12xx SIMATIC S7-15xx	Exclusion of local attackers and/or firmware update to V19 or later version
5	12/12/2023	Siemens	SSA-398330	Multiple Vulnerabilities in SIMATIC S7-1500 CPUs of GNU/Linux subsystem	All SEEPEX controls featuring the following SIEMENS hardware: SIMATIC S7-15xx	See SSA-398330
4	12/12/2023	Siemens	SSA-592380	Denial of Service Vulnerability in SIMATIC S7- 1500 CPUs via port 102 tcp	All SEEPEX controls featuring the following SIEMENS hardware: SIMATIC S7-15xx	Firmware update to V3.1.0 or later version
3	12/9/2023	Siemens	SSA-711309	Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Products	All SEEPEX controls on SIEMENS PLCs that are connected to a SEEPEX Gateway (e.g. SPG)	Firmware update to V8.1. SP1 or later version
2	11/14/2023	Siemens	SSA-699386	Multiple Vulnerabilities on SIEMENS SCALANCE Routern	All SEEPEX control cabinets featuring the following SIEMENS hardware: SCALANCE XB-200, XC- 200, XP-200, XF-200BA and XR-300WG	Firmware update to V4.5 or later version

1	5/28/2021	Siemens	SSA-434534	Memory Protection Bypass Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families	All SEEPEX controls featuring the following SIEMENS hardware: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP Open Controller CPU	SIMATIC S7-12xx: firmware update to V4.5 or later version SIMATIC S7-15xx: firmware update to V2.9.2 or later version