SEEPEX Sicherheitsupdates

Stand: 31. August 2026

Nr.	Datum des Bekanntwerdens	Quelle	Meldung	Auswirkung	Betroffenes SEEPEX Produkt	Handlungsempfehlung
88	8/11/2026	Schneider	CVE-2025-6625	Schneider Electric ist auf eine Schwachstelle in den folgenden Produkten aufmerksam geworden: Modicon M340, BMXNOR0200H: Modicon M340 X80 Ethernet-Kommunikationsmodule, BMXNGD0100: M580 Global Data-Modul, BMXNOC0401: Modicon M340 X80 Ethernet-Kommunikationsmodule, BMXNOE0100: Modicon M340 Modbus/TCP Ethernet-Modul sowie BMXNOE0110: Modicon M340 FactoryCast Modbus/TCP Ethernet-Modul. Wird die nachfolgend bereitgestellte Fehlerbehebung nicht angewendet, besteht das Risiko eines Denial-of-Service-Angriffs (DoS), der zur Nichtverfügbarkeit der betroffenen Geräte führen kann.	Modicon M340 BMXNOR0200H M580 Global Data module Modicon M340 X80 Ethernet Communication modules Modbus/TCP Ethernet Modicon M340 module	Es wird ein update auf die neuste Firmwareverion empfohlen
87	8/21/2026	Siemens	SSB-104599	Die aktuelle geopolitische Lage hat zu erhöhten Cybersicherheitsrisiken in allen Industriesektoren geführt. Dieses herausfordernde Umfeld wirkt sich auch auf die Landschaft der Betriebstechnologie (Operational Technology, OT) aus, in der wir eine Zunahme von Bedrohungsaktivitäten beobachten. Am 30.06.2025 veröffentlichten CISA, FBI, DC3 und NSA eine gemeinsame Warnmeldung über ein erhöhtes Bedrohungsniveau für kritische Infrastrukturen und industrielle Steuerungssysteme (ICS) [0]. Am 07.04.2026 wurde eine neue Warnmeldung veröffentlicht, in der nun zusätzlich Siemens S7-SPSen (Speicherprogrammierbare Steuerungen) als potenzielle Ziele genannt werden [1]. Anschließend wurde die bestehende Warnmeldung am 28.07.2026 aktualisiert, wobei die Siemens S7-1200 SPS nun ausdrücklich als spezifisches Ziel der laufenden Bedrohungskampagne hervorgehoben wird [1]. Am 19.08.2026 wurde eine weitere Warnmeldung veröffentlicht, die sich gezielt auf eine potenziell aktive Bedrohung gegen die speicherprogrammierbaren Steuerungen (SPS) der Siemens-S7-Serie konzentriert [10]. Angesichts dieser Entwicklungen empfiehlt Siemens seinen Kunden nachdrücklich, die notwendigen Maßnahmen zum Schutz ihrer Infrastruktur zu überprüfen und umzusetzen. Siemens unterstützt seine Kunden dabei mit seinem Angebot im Bereich Industrial Cybersecurity [11]. Für weitere Informationen wenden Sie sich bitte an Ihren Siemens-Vertriebsansprechpartner.	Siemens S7-1200 Gen1 Siemens S7-1200 Gen2 Siemens S7-1500	SICHERHEITSMASSNAHMEN Halten Sie Geräte und Systeme stets auf dem neuesten Softwarestand, um Angriffsvektoren zu begrenzen, die bekannte Schwachstellen ausnutzen könnten. Trennen Sie Geräte von Netzwerken mit unzureichendem Sicherheitsniveau (z. B. Internet, nicht gewartete interne Netzwerke oder physisch unzureichend gesicherte Umgebungen) oder setzen Sie zusätzliche Schutzmaßnahmen ein, beispielsweise Firewalls. Verwenden Sie starke und eindeutige Passwörter. Nutzen Sie keine Standardpasswörter und achten Sie auf ausreichend lange sowie komplexe Kennwörter. Befolgen Sie die Siemens Operational Guidelines for Industrial Security [2]. Ziehen Sie außerdem die gerätespezifische Benutzerdokumentation zu Rate, um stets informiert zu bleiben und mögliche Fehlkonfigurationen zu vermeiden [5][6][7][8][9].
86	8/11/2026	Siemens	SSA282044	Die Installationsprogramme, die für die Installation mehrerer Siemens-Produkte verwendet werden, sind von einer DLL-Hijacking-Schwachstelle betroffen. Diese könnte es einem Angreifer ermöglichen, beliebigen Code auszuführen, wenn ein berechtigter Benutzer eine Anwendung installiert, die die betroffene Installationskomponente verwendet. Das Risiko besteht ausschließlich während der Einrichtungs- und Installationsphase der betroffenen Anwendungen, die beispielsweise über OSD (Online Software Delivery) heruntergeladen werden. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, bei der Einrichtung und Installation stets die neuesten Versionen zu verwenden. Für weitere betroffene Produkte werden derzeit zusätzliche Korrekturversionen vorbereitet. Für Produkte, für die noch keine Korrekturen verfügbar sind, empfiehlt Siemens die Umsetzung spezifischer Gegenmaßnahmen, bis entsprechende Updates bereitgestellt werden.	SIMATIC S7-PLCSIM SIMATIC WinCC	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens nachdrücklich, den Netzwerkzugang zu Geräten durch geeignete Schutzmechanismen abzusichern. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security zu konfigurieren (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
85	8/11/2026	Siemens	SSA-392349	Mehrere industrielle Geräte enthalten eine Schwachstelle, die es einem Angreifer ermöglichen könnte, einen Denial-of-Service-Zustand (DoS) zu verursachen. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Für weitere betroffene Produkte werden derzeit zusätzliche Fehlerbehebungen vorbereitet. Für Produkte, für die noch keine Korrekturen verfügbar sind, empfiehlt Siemens die Umsetzung spezifischer Gegenmaßnahmen, bis entsprechende Updates bereitgestellt werden.	Scalance X-200 Familie Siemens S7-1200 Familie Siemens S7-1500 Familie	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens nachdrücklich, den Netzwerkzugang zu Geräten durch geeignete Schutzmechanismen abzusichern. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security zu konfigurieren (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity Für technische Dokumentationen oder Excel-Listen kann auch folgende, etwas formellere Fassung verwendet werden: Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf Geräte durch geeignete Sicherheitsmechanismen zu schützen. Für den Betrieb der Geräte in einer abgesicherten IT-Umgebung empfiehlt Siemens, die Umgebung gemäß den Siemens Operational Guidelines for Industrial Security zu konfigurieren (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) und die Empfehlungen in den jeweiligen Produkthandbüchern zu befolgen. Weitere Informationen zum Thema Industrial Security bei Siemens finden Sie unter: https://www.siemens.com/industrialsecurity.
84	14/07/2026	Siemens	SSA-828211	SIMATIC S7-PLCSIM Advanced weist eine Sicherheitslücke auf, die es einem Angreifer ermöglichen könnte, einen Denial-of-Service-Zustand herbeizuführen.	SIMATIC S7-PLCSIM Advanced All versions	Currently no fix is available
83	14/07/2026	Siemens	SSA-688146	SIMATIC S7-SPSen weisen mehrere Sicherheitslücken im Webserver auf, die es einem Angreifer ermöglichen könnten, Cross-Site-Scripting-Angriffe durchzuführen.	SIMATIC S7-1500 CPU family	Update to V2.9.9 or later version
82	14/07/2026	Rockwell Automation	CVE-2026-10573	Im 1734 POINT I/O™-Modul liegt eine Sicherheitslücke vor, die zu einem Denial-of-Service-Angriff führen kann. Die Sicherheitslücke resultiert aus der unsachgemäßen Verarbeitung speziell gestalteter CIP-Nachrichten, wodurch das Modul in einen Fehlerzustand geraten kann. Zur Wiederherstellung ist ein Neustart erforderlich.	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	In der Boot-Firmware der Controller 5380/5480/5580 mit einer Version unter 1.072 besteht eine Denial-of-Service-Sicherheitslücke. Diese Sicherheitslücke könnte es einem böswilligen Benutzer ermöglichen, ungültige Dateidaten auf den Controller zu schreiben, wodurch das Gerät in einen schwerwiegenden, nicht behebbaren Fehler (MNRF) gerät.	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	In den Controllern der Serien 5380, 5480 und 5580 besteht eine Denial-of-Service-Sicherheitslücke. Diese Sicherheitslücke könnte es einem böswilligen Benutzer ermöglichen, ungültige Dateidaten auf den Controller zu schreiben, wodurch das Gerät in einen schwerwiegenden, nicht behebbaren Fehler (MNRF) gerät.	CompactLogix® 5380 V35.011 or later	Corrected in Firmware Version 36.011 and later
79	14/07/2026	Rockwell Automation	SD1783	„In Studio 5000 Logix Designer® besteht eine Sicherheitslücke durch Pfadüberlauf, die auf eine unzureichende Begrenzung der Dateipfade in ACD-Projektdateien zurückzuführen ist. Die Software bereinigt oder validiert die in der ACD-Dateistruktur eingebetteten Dateinamen beim Öffnen des Projekts nicht, wodurch Pfadüberquerungssequenzen das vorgesehene Extraktionsverzeichnis umgehen können. Bei Ausnutzung dieser Schwachstelle könnte ein Angreifer eine bösartige ACD-Projektdatei erstellen, die dazu führt, dass beliebige Dateien an vom Angreifer kontrollierte Speicherorte im Dateisystem geschrieben werden, was möglicherweise zur Ausführung von Code führen kann. In Studio 5000 Logix Designer® besteht eine Sicherheitslücke, die die Ausführung von Remote-Code ermöglicht, da die Autorisierung für eine Konfigurationsdatei fehlerhaft ist. Dies kann es jedem authentifizierten Benutzer ermöglichen, die Pfade der in der Anwendung konfigurierten externen Tools zu ändern. Bei Ausnutzung dieser Schwachstelle könnte ein Angreifer die Konfiguration so ändern, dass sie auf eine bösartige ausführbare Datei verweist, was zur Ausführung von beliebigem Code führt, sobald ein Benutzer mit der Funktionalität der externen Tools interagiert. In Studio 5000 Logix Designer® besteht eine Sicherheitslücke, die die Ausführung von Code ermöglicht, da in der Konfiguration der externen Tools ein Suchpfad ohne Anführungszeichen angegeben ist. Die in der Konfigurationsdatei für externe Tools angegebenen Pfade zu ausführbaren Dateien sind nicht ordnungsgemäß in Anführungszeichen gesetzt, und da diese Pfade Leerzeichen enthalten, kann das Betriebssystem sie möglicherweise zu unbeabsichtigten ausführbaren Dateien auflösen, die in der Suchreihenfolge weiter vorne stehen. Bei Ausnutzung dieser Schwachstelle könnte ein Angreifer eine bösartige ausführbare Datei an einer Stelle innerhalb des Suchpfads platzieren, was zur Ausführung von beliebigem Code mit denselben Berechtigungen wie der Benutzer führt, der die Anwendung ausführt.	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	Bei den Kommunikationsmodulen CompactLogix® 5380, ControlLogix® 5580 und EN4TR besteht ein Sicherheitsproblem im Zusammenhang mit der Behandlung von widerrufenen CIP-Security-Zertifikaten. Das Sicherheitsproblem rührt daher, dass die Steuerung Zertifikate, die mit einem Zwischenzertifikat signiert wurden, das über eine Zertifikatssperrliste (CRL) gesperrt wurde, nicht ordnungsgemäß ablehnt. Dies könnte es einem Angreifer im Netzwerk ermöglichen, mithilfe eines Zertifikats, das als nicht vertrauenswürdig gelten sollte, eine Verbindung herzustellen und so möglicherweise die CIP-Security-Schutzmaßnahmen zu umgehen.	CompactLogix® 5380 V2 or later	Corrected in Firmware Version 38.011

77	6/6/2026	Siemens	SSA-674753	Siemens ET 200-Geräte weisen eine Denial-of-Service-Sicherheitslücke auf, die durch das Senden einer gültigen „Disconnect Request"-Nachricht (COTP DR TPDU) im S7-Protokoll ausgelöst werden kann. Dies führt dazu, dass das Gerät nicht mehr reagiert und zur Wiederherstellung des Betriebs ein Neustart erforderlich ist. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die noch keine Korrekturen verfügbar sind.	ET200	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf die Geräte durch geeignete Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für industrielle Sicherheit (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur industriellen Sicherheit von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
76	5/12/2026	Siemens	SSA-392349	Zahlreiche Industriegeräte weisen eine Sicherheitslücke auf, die es einem Angreifer ermöglichen könnte, einen Denial-of-Service-Zustand herbeizuführen. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens arbeitet derzeit an weiteren Korrekturversionen und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die noch keine Korrekturen verfügbar sind.	Industriegeräte IoT	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf die Geräte durch geeignete Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für industrielle Sicherheit (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur industriellen Sicherheit von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
75	4/14/2026	Siemens	SSA-599968	Eine Sicherheitslücke in den betroffenen Geräten könnte es einem Angreifer ermöglichen, einen Denial-of-Service-Angriff durchzuführen, wenn eine große Anzahl von Reset-Paketen des Profinet Discovery and Configuration Protocol (DCP) an die betroffenen Geräte gesendet wird. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Für Produkte, für die keine oder noch keine Korrekturen verfügbar sind, empfiehlt Siemens spezifische Gegenmaßnahmen.	PROFINET Devices	Siemens hat die folgenden spezifischen Abhilfemaßnahmen ermittelt, die Kunden anwenden können, um das Risiko zu verringern: Deaktivieren Sie Profinet in Produkten, bei denen Profinet optional ist und in Ihrer Umgebung nicht verwendet wird. Blockieren Sie eingehende Profinet Discovery and Configuration Protocol (DCP)-Pakete (Ethertype 0x8892, Frame-ID: 0xfefe) aus nicht vertrauenswürdigen Netzwerken. Produktspezifische Abhilfemaßnahmen oder Risikominderungen finden Sie im Abschnitt „Bekannte betroffene Produkte". Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen. ALLGEMEINE SICHERHEITEMPFEHLUNGEN Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf Geräte durch geeignete Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für industrielle Sicherheit (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur industriellen Sicherheit von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
73	3/10/2026	Rockwell Automation	CVE-2021-22681	Forscher haben festgestellt, dass die Software „Rockwell Automation Studio 5000 Logix Designer®" die Ermittlung eines kryptografischen Schlüssels ermöglichen könnte. Dieser interne Lizenzschlüssel wird von der Design-Software von Rockwell Automation für die Kommunikation mit Logix-Steuerungen verwendet. Bei erfolgreicher Ausnutzung könnte diese Sicherheitslücke es einer Anwendung eines Drittanbieters ermöglichen, eine Verbindung zu Logix-Steuerungen herzustellen. Um diese Sicherheitslücke auszunutzen, benötigt ein unbefugter Benutzer Netzwerkzugriff auf die Steuerung.	CompactLogix® 5380 v28 or later.	Installieren Sie den 1783-CSP CIP Security Proxy, um eine sichere Verbindung zwischen der Engineering-Workstation und der Steuerung herzustellen. Weitere Informationen finden Sie im Benutzerhandbuch zum 1783-CSP CIP Proxy.
72	3/19/2026	Siemens	SSA-452276	SIMATIC S7-1500-Geräte weisen eine Sicherheitslücke auf, die es einem Angreifer ermöglichen könnte, Code einzuschleusen, indem er einen legitimen Benutzer dazu verleitet, eine speziell gestaltete Trace-Datei über die Weboberfläche zu importieren.	SIMATIC S7-1500 CPU family	Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens arbeitet derzeit an weiteren Korrekturversionen und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die noch keine Korrekturen verfügbar sind.
71	2/18/2026	B&R	SA25P007	Es ist ein Update verfügbar, das eine veraltete Komponente eines Drittanbieters ersetzt, die von öffentlich bekannt gewordenen Sicherheitslücken in den oben aufgeführten Produktversionen betroffen ist. Obwohl bei Tests der betroffenen B&R-Produkte keine erfolgreiche Ausnutzung festgestellt wurde, könnten die identifizierten Sicherheitslücken potenzielle Angriffsvektoren darstellen, die unbefugten Zugriff, Datenoffenlegung oder die Ausführung von Remote-Code ermöglichen könnten.	Automation Studio < 6.5	Das Problem wurde in den folgenden Produktversionen behoben: B&R Automation Studio Version 6.5 B&R empfiehlt seinen Kunden, das Update so bald wie möglich zu installieren. Die Vorgehensweise zur Installation von Updates ist im Benutzerhandbuch beschrieben. Die Vorgehensweise zur Ermittlung der installierten Produktversion ist im Benutzerhandbuch beschrieben.
70	1/19/2026	B&R	SA25P004	In den ANSL- und OPC-UA-Clients der oben aufgeführten Produktversionen besteht eine Sicherheitslücke. Ein Angreifer könnte diese Sicherheitslücke ausnutzen, indem er sich als vertrauenswürdige Instanz ausgibt, wenn Automation Studio eine Verbindung zu einem ANSL- oder OPC-UA-Server herstellt. Die Schwerebewertung wurde unter Verwendung des FIRST Common Vulnerability Scoring System (CVSS)1 sowohl für v3.12 als auch für v4.03 durchgeführt. Die angegebenen Common Weakness Enumerations (CWE) wurden aus der MITRE CWE-Liste ausgewählt4	Automation Studio < 6.5	Das Problem wurde in den folgenden Produktversionen behoben: B&R Automation Studio Version 6.5 B&R empfiehlt seinen Kunden, das Update so bald wie möglich zu installieren. Die Vorgehensweise zur Installation von Updates ist im Benutzerhandbuch beschrieben. Die Vorgehensweise zur Ermittlung der installierten Produktversion ist im Benutzerhandbuch beschrieben.
69	1/13/2026	Siemens	SSA-674753	Siemens ET 200SP enthält eine Denial-of-Service-Sicherheitslücke, die durch das Senden einer gültigen S7-Protokoll-Trennungsanforderung (COTP DR TPDU) ausgelöst werden kann, wodurch das Gerät nicht mehr reagiert und ein Neustart erforderlich ist, um es wiederherzustellen. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	SIMATIC ET 200SP SIMATIC PN/PN Coupler	Siemens hat die folgenden spezifischen Maßnahmen identifiziert, mit denen Kunden das Risiko verringern können: Beschränken Sie den Zugriff auf das Netzwerk, in dem S7-Kommunikationsnachrichten ausgetauscht werden. Filtern Sie den Port 102 der Geräte so, dass nur Verbindungen zu/von den IP-Adressen von Maschinen akzeptiert werden, die vertrauenswürdig sind, z. B. mit einer externen Firewall.
68	Tuesday, December 9, 2025	Siemens	SSA-915282	Mehrere Industrieprodukte sind von einer Schwachstelle im Interniche IP-Stack betroffen. Die betroffenen Produkte führen in bestimmten Szenarien die TCP-Sequenznummernvalidierung nicht ordnungsgemäß durch, sondern akzeptieren Werte innerhalb eines breiten Bereichs. Dies könnte es einem nicht authentifizierten Angreifer ermöglichen, beispielsweise den Verbindungsaufbau zu stören, was möglicherweise zu einem Denial-of-Service führen kann. Der Angriff ist nur dann erfolgreich, wenn ein Angreifer IP-Pakete mit gefälschten Adressen zu genau abgestimmten Zeitpunkten einspeisen kann, und betrifft nur TCP-basierte Dienste.	SIMATIC ET 200SP SIMATIC PN/PN Coupler SIMATIC S7-1200 CPU V4 family SIMATIC S7-1500 family	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.
67	Tuesday, December 9, 2025	Siemens	SSA-800126	Betroffene Produkte desinfizieren benutzerkontrollierbare Eingaben beim Parsen von Dateien nicht ordnungsgemäß. Dies könnte es einem Angreifer ermöglichen, eine Typverwechslung zu verursachen und beliebigen Code innerhalb der betroffenen Anwendung auszuführen.	SIMATIC S7-PLCSIM Totally Integrated Automation Portal (TIA Portal)	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind. Siemens hat Produkte auf Basis des Totally Integrated Automation Portal (TIA Portal) V20 veröffentlicht, die nicht von CVE-2024-49849 betroffen sind. Weitere Informationen finden Sie im Kapitel „Zusätzliche Informationen" weiter unten.
66	Tuesday, December 9, 2025	Siemens	SSA-693808	Betroffene Produkte schränken die Zugriffsberechtigungen auf eine lokale Windows Named Pipe nicht ordnungsgemäß ein und bereinigen benutzerkontrollierte Eingaben, die an diese Named Pipe gesendet werden, nicht ordnungsgemäß. Dies könnte es einem lokal authentifizierten Angreifer ermöglichen, eine Typverwechslung zu verursachen und beliebigen Code innerhalb der betroffenen Anwendung und ihrer Berechtigungen auszuführen.	SIMATIC S7-PLCSIM V17 Totally Integrated Automation Portal (TIA Portal)	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.
65	Tuesday, December 9, 2025	Siemens	SSA-493396	Betroffene Produkte bereinigen benutzerkontrollierbare Eingaben beim Parsen von Projektdateien nicht ordnungsgemäß. Dies könnte es einem Angreifer ermöglichen, eine Typverwechslung zu verursachen und beliebigen Code innerhalb der betroffenen Anwendung auszuführen.	SIMATIC S7-PLCSIM V17 Totally Integrated Automation Portal (TIA Portal)	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.

64	Tuesday, December 9, 2025	Siemens	SSA-392859	Die betroffenen Produkte weisen eine Schwachstelle hinsichtlich der Ausführung von lokalem beliebigem Code auf, die es einem Angreifer ermöglichen könnte, Aktionen gegen	SIMATIC S7-PLCSIM Totally Integrated Automation Portal (TIA Portal)	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind. Siemens hat Produkte auf Basis des Totally Integrated Automation Portal (TIA Portal) V20 veröffentlicht, die nicht von CVE-2024-52051 betroffen sind. Weitere Informationen finden Sie im Kapitel „Zusätzliche Informationen" weiter unten.
63	Monday, December 8, 2025	Siemens	SSA-282044	Die Installationsprogramme, die zur Installation mehrerer Siemens-Produkte verwendet werden, sind von einer DLL-Hijacking-Sicherheitslücke betroffen. Diese könnte es einem Angreifer ermöglichen, beliebigen Code auszuführen, wenn ein legitimer Benutzer eine Anwendung installiert, die die betroffene Installationskomponente verwendet. Diese Sicherheitslücke stellt nur während der Einrichtungs- und Installationsphase der betroffenen Anwendungen ein Risiko dar, die beispielsweise über OSD (Online Software Delivery) heruntergeladen wurden.	Automation License Manager SIMATIC S7-PLCSIM SIMATIC WinCC TIA Administrator Totally Integrated Automation Portal (TIA Portal)	Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, bei der Einrichtung und Installation die neuesten Versionen zu verwenden. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.
62	Tuesday, November 11, 2025	Siemens	SSA-711309	Die OPC UA-Implementierungen (ANSI C und C++), die in mehreren SIMATIC-Produkten verwendet werden, enthalten eine Denial-of-Service-Sicherheitslücke, die es einem nicht authentifizierten Angreifer ermöglichen könnte, durch das Senden eines speziell gestalteten Zertifikats einen Denial-of-Service-Zustand zu erzeugen. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	SIMATIC WinCC	WORKAROUNDS UND ABHILFEMASSNAHMEN Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Deaktivieren Sie die OPC UA-Funktion, wenn sie nicht verwendet wird. Produktspezifische Abhilfemaßnahmen oder Abhilfemaßnahmen finden Sie im Abschnitt „Bekannte betroffene Produkte". Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
61	Tuesday, October 14, 2025	Rockwell Automation	SD 1757	Das EtherNet/IP-Kommunikationsmodul 1715 ist ein fehlertoleranter Adapter für Hochverfügbarkeitsanwendungen, der eine redundante E/A-Kommunikation über EtherNet/IP ermöglicht.	1715-AENTR EtherNet/IP Adapter	Abhilfemaßnahmen und Workarounds Kunden, die die betroffene Software verwenden und kein Upgrade auf eine der korrigierten Versionen durchführen können, sollten unsere Sicherheitsempfehlungen befolgen.
60	Tuesday, October 14, 2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500- und S7-1200-CPU-Versionen sind von einer offenen Redirect-Sicherheitslücke betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	SIMATIC S7-1500 SIMATIC S7-1200	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: • Klicken Sie nicht auf Links aus unbekannten Quellen. Produktspezifische Abhilfemaßnahmen oder Abhilfemaßnahmen finden Sie im Abschnitt „Bekannte betroffene Produkte". Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
59	Tuesday, October 14, 2025	Schneider Electrics	CVE-2024-6528	Schneider Electric ist eine Sicherheitslücke in seinen Modicon-Controllern M241 / M251, M258 / LMC058 und M262 bekannt. Die Modicon-Controller M241 / M251 / M258 / M262 und der Modicon Motion Controller LMC058 sind spezielle Steuerungen für leistungsintensive Anwendungen. Wenn die unten angegebene Abhilfemaßnahme nicht durchgeführt wird, besteht die Gefahr eines Cross-Site-Scripting- oder eines offenen Redirect-Angriffs, der zu einer Kontoübernahme oder zur Ausführung von Code im Browser des Benutzers führen könnte. Update Oktober 2025: Für die Modicon-Steuerungen M258 / LMC058 ist jetzt eine Abhilfemaßnahme verfügbar.	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	Wir empfehlen dringend die folgenden bewährten Verfahren für Cybersicherheit in der Industrie. • Platzieren Sie Netzwerke für Steuerungs- und Sicherheitssysteme sowie Remote-Geräte hinter Firewalls und isolieren Sie sie vom Unternehmensnetzwerk. • Installieren Sie physische Kontrollen, damit kein unbefugtes Personal auf Ihre industriellen Steuerungs- und Sicherheitssysteme , Komponenten, Peripheriegeräte und Netzwerke zugreifen kann. • Bewahren Sie alle Steuerungen in verschlossenen Schränken auf und lassen Sie sie niemals im „Programmiermodus". • Verbinden Sie Programmier-Software niemals mit einem anderen Netzwerk als dem für dieses Gerät vorgesehenen Netzwerk. • Scannen Sie alle Methoden des mobilen Datenaustauschs mit dem isolierten Netzwerk, wie z. B. CDs, USB-Sticks usw., vor der Verwendung in den Terminals oder an einem mit diesen Netzwerken verbundenen Knotenpunkt. • Lassen Sie niemals zu, dass mobile Geräte, die mit einem anderen als dem vorgesehenen Netzwerk verbunden waren, ohne ordnungsgemäße Bereinigung eine Verbindung zu den Sicherheits- oder Steuerungsnetzwerken herstellen. • Minimieren Sie die Netzwerkexposition für alle Steuerungssystemgeräte und -systeme und stellen Sie sicher, dass sie nicht über das Internet zugänglich sind. • Wenn ein Fernzugriff erforderlich ist, verwenden Sie sichere Methoden wie virtuelle private Netzwerke (VPNs). Beachten Sie, dass VPNs Schwachstellen aufweisen können und auf die aktuellste verfügbare Version aktualisiert werden sollten . Beachten Sie außerdem, dass VPNs nur so sicher sind wie die angeschlossenen Geräte. Weitere Informationen finden Sie im Dokument „Empfohlene Best Practices für Cybersicherheit" von Schneider Electric.
58	Tuesday, September 9, 2025	Siemens	SSA-503939	Im BIOS des SIMATIC S7-1500 TM MFP wurden mehrere Sicherheitslücken entdeckt. Siemens arbeitet derzeit an Korrekturversionen und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die noch keine oder noch keine Korrekturen verfügbar sind.	SIMATIC S7-1500 TM MFP - BIOS	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Erstellen und führen Sie nur Anwendungen aus vertrauenswürdigen Quellen aus. Befolgen Sie bitte die allgemeinen Sicherheitsempfehlungen.
57	Tuesday, September 9, 2025	Siemens	SSA-691715	Die Modicon-Controller M241 / M251 / M258 / M262 und der Modicon Motion Controller LMC058 sind	OpenPCS 7 V9.1 SIMATIC NET PC Software SIMATIC WinCC SIMATIC WinCC Runtime Professional SIMATIC WinCC Unified PC Runtime V18	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Aktualisieren Sie den zugrunde liegenden OPC Foundation Unified Architecture Local Discovery Server (UA-LDS) nach Möglichkeit auf V1.04.405 oder höher. Produktspezifische Abhilfemaßnahmen oder Abhilfemaßnahmen finden Sie im Abschnitt „Bekannte betroffene Produkte". Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
56	Thursday, August 14, 2025	Rockwell Automation	SD 1734	spezielle Steuerungen für leistungsintensive Anwendungen.	Studio 5000 Logix Designer 36.00.02	Abhilfemaßnahmen und Workarounds Benutzer sollten nach Möglichkeit auf die korrigierte Version aktualisieren. Wenn Benutzer, die die betroffene Software verwenden, kein Upgrade der Version durchführen können, sollten bewährte Sicherheitsverfahren angewendet werden.
55	Thursday, August 14, 2025	Rockwell Automation	SD 1732	Wenn die unten angegebene Abhilfemaßnahme nicht durchgeführt wird, besteht die Gefahr eines Cross-Site-Scripting- oder eines offenen Redirect-Angriffs,	1756-EN2T/D,1756-EN2F/C, 1756-EN2TR/C, 1756-EN3TR/B, 1756-EN2TP/A Version 11.004 or below	Abhilfemaßnahmen und Workarounds Benutzer sollten nach Möglichkeit auf die korrigierte Version aktualisieren. Wenn Benutzer, die die betroffene Software verwenden, kein Upgrade der Version durchführen können, sollten bewährte Sicherheitsverfahren angewendet werden.

54	Tuesday, August 12, 2025	Schneider Electrics	CVE-2025-6625	der zu einer Kontoübernahme oder zur Ausführung von Code im Browser des Benutzers führen könnte.	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	Wir empfehlen dringend die folgenden bewährten Verfahren für Cybersicherheit in der Industrie. • Platzieren Sie Netzwerke von Steuerungs- und Sicherheitssystemen sowie Remote-Geräte hinter Firewalls und isolieren Sie sie vom Unternehmensnetzwerk. • Installieren Sie physische Kontrollen, damit kein unbefugtes Personal auf Ihre industriellen Steuerungs- und Sicherheitssysteme, Komponenten, Peripheriegeräte und Netzwerke zugreifen kann. Sicherheitsmitteilung von Schneider Electric 12. August 2025 Dokumentreferenznummer – SEVD-2025-224-05 Seite 4 von 5 Öffentlich / TLP: Freigegeben • Bewahren Sie alle Steuerungen in verschlossenen Schränken auf und lassen Sie sie niemals im „Programm“-Modus. • Verbinden Sie Programmiersoftware niemals mit einem anderen Netzwerk als dem für dieses Gerät vorgesehenen Netzwerk. • Scannen Sie alle Methoden des mobilen Datenaustauschs mit dem isolierten Netzwerk, wie z. B. CDs, USB-Sticks usw., vor der Verwendung in den Terminals oder an einem mit diesen Netzwerken verbundenen Knoten. • Lassen Sie niemals zu, dass mobile Geräte, die mit einem anderen als dem vorgesehenen Netzwerk verbunden waren, ohne ordnungsgemäße Bereinigung eine Verbindung zu den Sicherheits- oder Steuerungsnetzwerken herstellen. • Minimieren Sie die Netzwerkexposition für alle Steuerungssystemgeräte und -systeme und stellen Sie sicher, dass sie nicht über das Internet zugänglich sind. • Wenn ein Fernzugriff erforderlich ist, verwenden Sie sichere Methoden wie Virtual Private Networks (VPNs). Beachten Sie, dass VPNs Schwachstellen aufweisen können und auf die aktuellste verfügbare Version aktualisiert werden sollten. Beachten Sie außerdem, dass VPNs nur so sicher sind wie die angeschlossenen Geräte. Weitere Informationen finden Sie in den von Schneider Electric empfohlenen Cybersicherheitsmaßnahmen.
53	Tuesday, August 12, 2025	Schneider Electrics	CVE-2024-5056	Update Oktober 2025: Für die Modicon-Steuerungen M258 / LMC058 ist jetzt eine Abhilfemaßnahme verfügbar.	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	Allgemeine Sicherheitsempfehlungen Wir empfehlen dringend die folgenden bewährten Verfahren für Cybersicherheit in der Industrie. • Platzieren Sie Netzwerke für Steuerungs- und Sicherheitssysteme sowie Remote-Geräte hinter Firewalls und isolieren Sie sie vom Unternehmensnetzwerk. • Installieren Sie physische Kontrollen, damit kein unbefugtes Personal auf Ihre industriellen Steuerungs- und Sicherheitssysteme, Komponenten, Peripheriegeräte und Netzwerke zugreifen kann. • Bewahren Sie alle Steuerungen in verschlossenen Schränken auf und lassen Sie sie niemals im „Programm“-Modus. • Verbinden Sie Programmier-Software niemals mit einem anderen Netzwerk als dem für dieses Gerät vorgesehenen Netzwerk. • Scannen Sie alle Methoden des mobilen Datenaustauschs mit dem isolierten Netzwerk, wie z. B. CDs, USB-Sticks usw., bevor Sie sie in den Terminals oder anderen mit diesen Netzwerken verbundenen Knoten verwenden. • Lassen Sie niemals zu, dass mobile Geräte, die mit einem anderen Netzwerk als dem vorgesehenen Netzwerk verbunden waren, ohne ordnungsgemäße Bereinigung eine Verbindung zu den Sicherheits- oder Steuerungsnetzwerken herstellen. Sicherheitsmitteilung von Schneider Electric 24. Juni 2011 (25. August 2012) Dokumentreferenznummer – SEVD-2024-163-01(v2.0.0) Seite 4 von 5 Öffentlich / TLP: Freigegeben • Minimieren Sie die Netzwerkexposition für alle Steuerungssystemgeräte und -systeme und stellen Sie sicher, dass sie nicht über das Internet zugänglich sind. • Wenn ein Fernzugriff erforderlich ist, verwenden Sie sichere Methoden wie virtuelle private Netzwerke (VPNs). Beachten Sie, dass VPNs Schwachstellen aufweisen können und auf die aktuellste verfügbare Version aktualisiert werden sollten. Beachten Sie außerdem, dass VPNs nur so sicher sind wie die angeschlossenen Geräte.
52	Monday, August 18, 2025	Siemens	SSA-711309		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 hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Deaktivieren Sie die OPC UA-Funktion, wenn sie nicht verwendet wird. Produktspezifische Abhilfemaßnahmen oder Entschärfungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen.
51	Tuesday, August 12, 2025	Siemens	SSA-460466		Totally Integrated Automation Portal (TIA Portal) V18 & V20	Produktspezifische Abhilfemaßnahmen oder Schutzmaßnahmen finden Sie im Abschnitt „Bekannte betroffene Produkte“. Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
50	Tuesday, August 12, 2025	Siemens	SSA-353002	Die SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Familie ist von mehreren Sicherheitslücken betroffen. CVE-2023-44318 und CVE-2023-44321 wurden zuvor als Teil von SSA-699386 veröffentlicht.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Familie.	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugang zu den Geräten mit geeigneten Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu beachten. Weitere Informationen zu Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
49	Tuesday, August 12, 2025	Siemens	SSA-800126	Betroffene Produkte bereinigen benutzerkontrollierbare Eingaben beim Parsen von Dateien nicht ordnungsgemäß. Dies könnte es einem Angreifer ermöglichen, eine Typverwechslung zu verursachen und beliebigen Code innerhalb der betroffenen Anwendung auszuführen. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind. Siemens hat Produkte auf Basis des Totally Integrated Automation Portal (TIA Portal) V20 veröffentlicht, die nicht von CVE-2024-49849 betroffen sind. Weitere Informationen finden Sie im Kapitel „Zusätzliche Informationen“ weiter unten.	SIMATIC S7-PLCSIM V16 Totally Integrated Automation Portal V16, V17, V18 (TIA Portal)	WORKAROUNDS UND ABHILFEMASSNAHMEN Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: CVE-2024-49849: Vermeiden Sie das Öffnen nicht vertrauenswürdiger Dateien aus unbekannten Quellen in betroffenen Produkten.
48	Monday, July 21, 2025	Siemens	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	
47	Tuesday, July 8, 2025	Siemens	SSA-460466	Eine Schwachstelle in TIA Project Server und TIA Portal könnte es einem Angreifer ermöglichen, einen Denial-of-Service-Zustand herbeizuführen.	Totally Integrated Automatin Portal (TIA Portal) V18 & V20	V18: Currently no fix is available V20: Update to V20 Update 3 or later version
46	Tuesday, July 8, 2025	Siemens	SSA-573669	Siemens TIA Administrator vor Version 3.0.6 enthält mehrere Schwachstellen, die es einem Angreifer ermöglichen könnten, während der Installation Berechtigungen zu erweitern oder beliebigen Code auszuführen.	TIA Administrator All versions < 3.0.6	Update to V3.0.6 or later version

45	Tuesday, July 8, 2025	Siemens	SSA-593272	In den betroffenen Produkten besteht eine Schwachstelle, die es Angreifern unter bestimmten Umständen ermöglichen könnte, die Verfügbarkeit der Geräte zu beeinträchtigen. Der zugrunde liegende TCP-Stack kann dazu gezwungen werden, für jedes eingehende Paket sehr rechenintensive Aufrufe durchzuführen, was zu einem Denial-of-Service führen kann. rvice.	SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0) All versions >= V4.2.0 SIMATIC S7-1200 CPU family (incl. SIPLUS variants) All versions < V4.4.0 SIMATIC S7-1500 CPU family (incl. related ET 200 CPUs and SIPLUS variants)	Currently no fix is planned Update to V4.5.2 or later version Update to V2.8 or later version
44	Tuesday, July 8, 2025	Siemens	SSA-614723	Die Siemens User Management Component (UMC) ist von drei Sicherheitslücken betroffen, die es einem nicht authentifizierten Angreifer ermöglichen könnten, einen Denial-of-Service-Zustand herbeizuführen.	Totally Integrated Automation Portal (TIA Portal) V18 & V20	V18: Update UMC to V2.15.1.1 or later compatible version V20: Update UMC to V2.15.1.1 or later compatible version
43	Tuesday, July 8, 2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500- und S7-1200-CPU-Versionen sind von einer Open-Redirect-Sicherheitslücke betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken.	SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.7	Update to V4.7 or later version
42	Tuesday, June 10, 2025	Siemens	SSA-858251	Die unten aufgeführten Produkte enthalten zwei Schwachstellen zur Umgehung der Authentifizierung, die es einem Angreifer ermöglichen könnten, Zugriff auf die vom Server verwalteten Daten zu erhalten. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Korrekturversionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die noch keine oder noch keine Korrekturen verfügbar sind.	OPC UA	UMGEHUNGEN UND ABHILFEMASSNAHMEN Produktspezifische Abhilfemaßnahmen oder Milderungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen. ALLGEMEINE SICHERHEITSEMPFEHLUNGEN Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf Geräte mit geeigneten Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Betriebsrichtlinien von Siemens für industrielle Sicherheit (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu befolgen. Weitere Informationen zur industriellen Sicherheit von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity WORKAROUNDS AND MITIGATIONS 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
41	05/13/2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500 und S7-1200 CPU Versionen sind von einer offenen Redirect-Schwachstelle betroffen die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. vom Angreifer gewählten URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt ein Update auf die neuesten Versionen. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	SIMATIC S7-1200 / S7-1500 CPU	Siemens hat die folgenden spezifischen Umgehungslösungen und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: - Klicken Sie nicht auf Links von unbekannten Quellen. Produktspezifische Abhilfemaßnahmen oder Mitigations finden Sie im Abschnitt Betroffene Produkte und Lösung. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen. ALLGEMEINE SICHERHEITSEMPFEHLUNGEN Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf Geräte mit geeigneten Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung betreiben zu können, empfiehlt Siemens Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens die Konfiguration der Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren, und den Empfehlungen in den Produkthandbüchern zu folgen. Weitere Informationen zu Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurit
40	Tuesday, May 13, 2025	Siemens	SSA-054046	Mehrere SIMATIC S7-1500 CPU-Versionen sind von einer Authentifizierungs-Bypass-Schwachstelle betroffen, die es einem nicht authentifizierten Angreifer ermöglichen könnte, Kenntnisse über tatsächliche und konfigurierte maximale Zykluszeiten und Kommunikationslast der CPU zu erlangen. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt ein Update auf die neuesten Versionen. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die noch keine Fixes verfügbar sind.	SIMATIC S7-1500 CPU SIMATIC ET 200SP	Produktspezifische Abhilfemaßnahmen oder Milderungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen. ALLGEMEINE SICHERHEITSEMPFEHLUNGEN Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugriff auf Geräte mit geeigneten Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu beachten. Weitere Informationen zu Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity

39	Tuesday, April 8, 2025	Schneider Electric	CVE-2024-8936	Schneider Electric hat Kenntnis von mehreren Sicherheitslücken in seinen Modicon Controllern M340 / Momentum / MC80 Produkten bekannt. Modicon PAC steuern und überwachen industrielle Abläufe. Werden die unten aufgeführten Abhilfemaßnahmen nicht befolgt, besteht die Gefahr, dass Unbefugte auf den Controller zugreifen, was Dies kann zu einem möglichen Denial-of-Service und einem Verlust der Vertraulichkeit und Integrität des Controllers führen. April 2025 Update: Eine Abhilfemaßnahme ist jetzt für den Modicon Momentum Unity M1E Processor verfügbarVersion prior to SV3.65	Modicon M340 CPU (part numbers BMXP34*)	Die Version SV3.65 der Mod-icon M340-Firmware enthält einen Fix für diese Sicherheitslücken
38	Tuesday, April 8, 2025	Schneider Electric	CVE-2020-28895	Schneider Electric ist über mehrere Sicherheitslücken bei der Speicherzuweisung mit der Bezeichnung „BadAlloc" informiert, die von Microsoft am 29. April 2021 bekannt gegeben wurden. Die Auswirkungen einer erfolgreichen Ausnutzung der Schwachstellen können je nach Kontext zu einer Denial-of-Service oder Remotecodeausführung führen, je nach Kontext. Update vom April 2025: Eine Abhilfemaßnahme ist für BMECRA31210, BMXCRA31200, BMXCRA31210 (Seite 13) und die Abhilfemaßnahmen für dieses Produkt wurden aktualisiert.	Modicon M340 CPU (BMXP34*) v3.40 und vorherige	Die Version 3.50 von Modicon M340 enthält einen Fix für diese Sicherheitslücken
37	Tuesday, April 8, 2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500 und S7-1200 CPU-Versionen sind von einer offenen Umleitungsschwachstelle betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer zu einer vom Angreifer gewählten URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken.	SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.7	Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.
36	Tuesday, April 8, 2025	Siemens	SSA-725549	In den betroffenen Produkten besteht eine Schwachstelle, die es entfernten Angreifern ermöglichen könnte, die Verfügbarkeit der Geräte unter bestimmten Bedingungen zu beeinflussen	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 hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.
35	Tuesday, April 8, 2025	Siemens	SSA-195895	Der Webserver mehrerer SIMATIC-Produkte ist von einer Benutzeraufzählungsschwachstelle betroffen, die es einem nicht authentifizierten Angreifer ermöglichen könnte, gültige Benutzernamen zu identifizieren.	SIMATIC S7-1200 CPU 1215C DC/DC/DC (6ES7215-1AG40-0XB0) All versions < V4.7	Siemens hat neue Versionen für die betroffenen Produkte veröffentlicht und empfiehlt ein Update auf die neuesten Versionen.
34	Tuesday, March 11, 2025	Siemens	SSA-858251	Die unten aufgeführten Produkte enthalten zwei Schwachstellen zur Umgehung der Authentifizierung, die es einem Angreifer ermöglichen könnten, Zugriff auf die vom Server verwalteten Daten zu erhalten. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die keine Fixes oder noch keine verfügbar sind.	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.
33	Tuesday, March 11, 2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500- und S7-1200-CPU-Versionen sind von einer offenen Umleitungsschwachstelle betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	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
32	Tuesday, March 11, 2025	Siemens	SSA-054046	Mehrere SIMATIC S7-1500 CPU-Versionen sind von einer Authentifizierungs-Bypass-Schwachstelle betroffen, die es einem nicht authentifizierten Angreifer ermöglichen könnte, Kenntnisse über tatsächliche und konfigurierte maximale Zykluszeiten und Kommunikationslast der CPU zu erlangen. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt ein Update auf die neuesten Versionen. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die keine Fixes oder noch keine verfügbar sind.	X	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	Tuesday, February 11, 2025	Schneider	Vulnerabilities Details	Schneider Electric hat Kenntnis von mehreren Schwachstellen in seinen Modicon Controller Produkten. Die Modicon Programmable Automation Controller werden für komplexe vernetzte Kommunikations-, Anzeige- und Steuerungsanwendungen verwendet Wenn die unten aufgeführten Abhilfemaßnahmen nicht angewendet werden, besteht die Gefahr, dass unaufgeforderte Befehle auf der SPS ausgeführt werden, was zu einem Verlust der Verfügbarkeit des Controllers führen kann	Modicon Controller M340, M580	Update Software and Firmware and Rebuild the Projects

30	Tuesday, February 11, 2025	Siemens	SSA-195895	Der Webserver mehrerer SIMATIC-Produkte ist von einer Schwachstelle in der Benutzeraufzählung betroffen, die es einem nicht authentifizierten Angreifer ermöglichen könnte, gültige Benutzernamen zu ermitteln. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die Fixes nicht oder noch nicht verfügbar sind.	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
29	Tuesday, February 11, 2025	Siemens	SSA-224824	Die SIMATIC S7-1200 CPU-Familie vor V4.7 ist von zwei Denial-of-Service-Schwachstellen betroffen. Siemens hat neue Versionen für die betroffenen Produkte veröffentlicht und empfiehlt ein Update auf die neuesten Versionen.	SIMATIC S7-1200 CPU family V4 (incl. SIPLUS variants)	Update to V4.7 or later version
28	Tuesday, February 11, 2025	Siemens	SSA-342348	Betroffene Produkte machen Benutzersitzungen beim Abmelden nicht korrekt ungültig. Dies könnte es einem nicht authentifizierten Angreifer, der das Sitzungs-Token auf andere Weise erlangt hat, ermöglichen, die Sitzung eines legitimen Benutzers auch nach der Abmeldung wieder zu verwenden. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	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
27	Tuesday, February 11, 2025	Siemens	SSA-349422	Eine Schwachstelle in den betroffenen Produkten könnte es einem unbefugten Angreifer mit Netzwerkzugang ermöglichen, einen Denial-of-Service-Angriff durchzuführen, der zum Verlust der Echtzeitsynchronisation führt. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	SIMATIC ET 200SP IM 155-6 PN HF (incl. SIPLUS variants)	Update to V4.2.0 or later version
26	Tuesday, February 11, 2025	Siemens	SSA-712929	Eine Schwachstelle in der openSSL-Komponente (CVE-2022-0778, [0]) könnte es einem Angreifer ermöglichen, einen Denial-of-Service-Zustand herbeizuführen, indem er speziell gestaltete Elliptic-Curve-Zertifikate für Produkte bereitstellt, die eine anfällige Version von openSSL verwenden. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die noch keine Fixes verfügbar sind.	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
25	Tuesday, January 14, 2025	Siemens	SSA-876787	Mehrere SIMATIC S7-1500- und S7-1200-CPU-Versionen sind von einer offenen Umleitungsschwachstelle betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	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 hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Klicken Sie nicht auf Links von unbekannten Quellen. Produktspezifische Abhilfemaßnahmen oder Mitigations finden Sie im Abschnitt Betroffene Produkte und Lösung. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen.
24	Tuesday, January 14, 2025	Siemens	SSA-730482	Eine Schwachstelle im Anmeldedialog von SIMATIC WinCC könnte es einem lokalen Angreifer ermöglichen, einen Denial-of-Service-Zustand in der Laufzeit des SCADA-Systems zu verursachen. Siemens hat neue Versionen für die betroffenen Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren.	SIMATIC WinCC Runtime Professional SIMATIC PCS 7	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Aktivieren Sie SIMATIC Logon im User Administrator der SIMATIC PCS 7 Operator Stations Produktspezifische Abhilfemaßnahmen oder Abschwächungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen.
23	Tuesday, January 14, 2025	Siemens	SSA-711309	Die OPC UA-Implementierungen (ANSI C und C++), die in mehreren SIMATIC-Produkten verwendet werden, enthalten eine Denial-of-Service-Schwachstelle, die es einem nicht authentifizierten Angreifer ermöglichen könnte, durch Senden eines speziell gestalteten Zertifikats einen Denial-of-Service-Zustand zu erzeugen. Siemens hat neue Versionen für mehrere betroffene Produkte herausgegeben und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Korrekturen verfügbar sind.	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 hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Deaktivieren Sie die OPC UA-Funktion, wenn sie nicht verwendet wird. Produktspezifische Abhilfemaßnahmen oder Entschärfungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen.
22	Tuesday, January 14, 2025	Siemens	SSA-413565	Mehrere SCALANCE-Geräte sind von mehreren Schwachstellen betroffen, die es einem Angreifer ermöglichen könnten, Code einzuschleusen, Daten als Debug-Informationen sowie CLI-Benutzerpasswörter abzurufen oder die CLI in einen nicht reagierenden Zustand zu versetzen. Siemens hat Updates für die betroffenen Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG family	Produktspezifische Abhilfemaßnahmen oder Entschärfungen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte beachten Sie die allgemeinen Sicherheitsempfehlungen.

21	Tuesday, December 10, 2024	Siemens	SSA-711309	Die OPC UA-Implementierungen (ANSI C und C++), die in mehreren SIMATIC-Produkten verwendet werden, enthalten eine Denial-of-Service-Schwachstelle, die es Angreifer ermöglichen könnte, durch Senden eines speziell gestalteten Zertifikats einen Denial-of-Service zu erzeugen. Siemens hat für mehrere betroffenen Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	SIMATIC S7-1500 CPU-Familie (inkl. zugehörige ET200 CPUs und SIPLUS-Varianten) SIMATIC WinCC OP UA Client SIMATIC WinCC Runtime Professional SIMATIC WinCC Unified OPC UA ServerSIMATIC 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	Aktualisierung auf V2.0.0.1 oder höher Weitere Informationen hier.
20	Tuesday, December 10, 2024	Siemens	SSA-876787	Mehrere SIMATIC S7-1500 und S7-1200 CPU-Versionen sind von einer offenen Redirect-Schwachstelle betroffen, die es einem Angreifer ermöglichen könnte, den Webserver der betroffenen Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer gewählte URL umzuleiten. Für einen erfolgreicehn Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat für mehrere betroffenen Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	SIMATIC S7-1500 Software Controller	Derzeit ist keine Lösung verfügbar. Weitere Informationen hier.
19	Tuesday, November 12, 2024	Siemens	SSA-871035	Betroffene Produkte bereinigen benutzerkontrollierte Eingaben beim Parsen von Dateien nicht richtig. Die könnte einem Angreifer ermöglichen, eine Typverwechslung herbeizuführen und beliebigen Code innerhalb der betroffenen Anwendung auszuführen. Siemens hat neue Versionen für mehrere Produkte veröffentlicht und empfiehlt ein Update auf die neuesten Versionen. Siemens bereitet weitere Fix-Versionen vor und empfhiehlt Gegenmaßnahmen für Produkte, für die keine oder noch keine Fixes verfügbar sind.	SIMATIC S7-PLCSIM V16 Totally Integrated Automation Portal V16, V17, V18 (TIA Portal)	Derzeit ist keine Lösung geplant. Weitere Informationen hier.
18	Tuesday, October 8, 2024	Siemens	SSA-054046	Mehrere Versionen der SIMATIC S7-1500 CPU sind von einer Sicherheitslücke bei der Umgehung der Authentifizierung betroffen, die es einem nicht authentifizierten Remote-Angreifer ermöglichen könnte, Informationen über die tatsächlichen und konfigurierten maximalen Zykluszeiten und die Kommunikationslast der CPU zu erhalten. Siemens hat für mehrere betroffene Produkte neue Versionen veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt Gegenmaßnahmen für Produkte, für die Fixes nicht oder noch nicht verfügbar sind.	Alle S7-1500 CPUs	Produktspezifische Abhilfemaßnahmen oder Risikominderungen finden Sie im Abschnitt „Betroffene Produkte und Lösungen“. Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
17	Tuesday, October 8, 2024	Siemens	SSA-876787	Mehrere CPU-Versionen von SIMATIC S7-1500 und S7-1200 sind von einer offenen Umleitungsschwachstelle betroffen, die es einem Angreifer ermöglichen könnte, den Webserver betroffener Geräte dazu zu bringen, einen legitimen Benutzer auf eine vom Angreifer ausgewählte URL umzuleiten. Für einen erfolgreichen Angriff muss der legitime Benutzer aktiv auf einen vom Angreifer erstellten Link klicken. Siemens hat neue Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens bereitet weitere Fix-Versionen vor und empfiehlt spezifische Gegenmaßnahmen für Produkte, für die Fixes nicht oder noch nicht verfügbar sind.	Simatic S7-1200 Familie Simatic S7-1500 Familie	Siemens hat die folgenden spezifischen Workarounds und Minderungsmaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Klicken Sie nicht auf Links aus unbekannten Quellen. Produktspezifische Abhilfemaßnahmen oder Minderungsmaßnahmen finden Sie im Abschnitt Betroffene Produkte und Lösungen. Bitte befolgen Sie die allgemeinen Sicherheitsempfehlungen.
16	Tuesday, August 13, 2024	Rockwell Automation	SD 1685	Denial-of-Service-Schwachstelle über Eingabevalidierung. Diese Schwachstelle tritt auf, wenn eine fehlerhafte PCCC-Nachricht empfangen wird, dienen Fehler in der Steuerung verursacht.	ControlLogix/GuardLogix 5580 und Compact-Logix/Compact GuardLogix® 5380 Steuerung	Aktualisierung auf die neueste Firmware-Version. Beschränkung der Kommunikation auf CIP_Objekt 103 (0x67)
15	Tuesday, August 13, 2024	Rockwell Automation	SD 1685	Denial-of-Service-Schwachstelle über Eingabevalidierung. Ein fehlerhaftes PTP-Management-Paket kann einen schwerwiegenden nicht behebbaren Fehler in der Steuerung verursachen.	ControlLogix/GuardLogix 5580 und Compact-Logix/Compact GuardLogix® 5380 Steuerung	Aktualisierung auf die neueste Firmware-Version. Wenn PTP-Nachrichten nicht verwendet werden, blockieren Sie auf der Netzwerkebene den Port UDP 319/320
14	Tuesday, July 9, 2024	Siemens	SSA-779936	Betroffene Anwendungen schränken den .NET Binary-Formatter beim Deserialisieren benutzersteuerbarer Eingaben nicht richtig ein. Dies könnte einem Angreifer ermöglichen, eine Typverwechslung zu verursachen und beliebigen Code innerhalb der betroffenen Anwendung auszuführen.	Totally Ingegrated Automation Portal (TIA Portal) V19 und älter	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu reduzieren: Vermeiden Sie das Öffnen nicht vertrauenswürdiger Dateien aus unbekannten Quellen in betroffenen Produkten
13	Tuesday, July 9, 2024	Siemens	SSA-473245	Eine Schwachstelle in betroffenen Geräten könnte einem Angreifer einen Denial-of-Service Angriff ermöglichen, wenn eine große Menge speziell gestalteter UDP-Pakete an das Gerät gesendet wird. Siemens hat neuen Versionen für mehrere betroffene Produkte veröffentlicht und empfiehlt, auf die neuesten Versionen zu aktualisieren. Siemens empfiehlt spezifische Gegenmaßnahmen für Produkte, für die Fixes nicht oder noch nicht verfügbar sind.	Simatic S7-1200 CPU Family, Simatic S7-1500 Family, ET200SP	Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu reduzieren: Netzwerkzugriff auf betroffene Geräte einschränken
12	Tuesday, June 11, 2024	Siemens	SSA-319319	TIA Administrator erstellt temporäre Download-Dateien in einem Verzeichnis mit unsicheren Berechtigungen. Dies könnte es jedem authentifizierten Angreifer unter Windows ermöglichen, den Update-Prozess zu unterbrechen.	TIA-Administrator <3.2	Siemens hat eine neue Version von TIA-Administrator veröffentlicht und empfiehlt, auf die neueste Version zu aktualisieren. Siemens hat die folgenden spezifischen Workarounds und Abhilfemaßnahmen identifiziert, die Kunden anwenden können, um das Risiko zu verringern: Entfernen Sie die Schreibberechtigung für nicht-administrative Benutzer für Dateien und Ordner, die sich unter dem Installationspfad befinden.

11	Tuesday, June 11, 2024	Siemens	SSA-353002	Die SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Familie ist von mehreren Sicherheitslücken betroffen. CVE-2023-44318 und CVE-2023-44321 wurden zuvor als Teil von SSA-699386 veröffentlicht.	SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Familie.	Als allgemeine Sicherheitsmaßnahme empfiehlt Siemens dringend, den Netzwerkzugang zu den Geräten mit geeigneten Mechanismen zu schützen. Um die Geräte in einer geschützten IT-Umgebung zu betreiben, empfiehlt Siemens, die Umgebung gemäß den Siemens-Betriebsrichtlinien für Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) zu konfigurieren und die Empfehlungen in den Produkthandbüchern zu beachten. Weitere Informationen zu Industrial Security von Siemens finden Sie unter: https://www.siemens.com/industrialsecurity
10	Tuesday, June 11, 2024	Siemens	SSA-711309	Denial-of-Service-Schwachstelle in den OPC UA-Implementierungen von SIMATIC-Produkten	Alle SEEPEX Steuerungen mit folgender SIEMENS Software: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP	Derzeit keine Lösung verfügbar/ Update auf die neueste Version
9	Tuesday, May 21, 2024	Rockwell Automation	SD1672	WICHTIGER HINWEIS: Rock-well Automation wieder-holt die Anweisung an seine Kunden, Geräte vom Inter-net zu trennen, um sich vor Cyber-Bedrohungen zu schützen Aufgrund erhöhter geopoli-tischer Spannungen und feindlicher Cyber-Aktivitä-ten auf der ganzen Welt fordert Rockwell Automa-tion alle Kunden auf, SO-FORT zu prüfen, ob ihre Ge-räte mit dem öffentlichen Internet verbunden sind, und, falls dies der Fall ist, diese Verbindung für Ge-räte, die nicht speziell für eine öffentliche Internet-verbindung ausgelegt sind, dringend zu entfernen.	Alle SEEPEX Steuerungen mit Rockwell Automation HardwareAll SEEPEX controls with Rockwell Automation Hardware	Aufgrund erhöhter geopolitischer Spannungen und feindlicher Cyber-Aktivitäten auf der ganzen Welt fordert Rockwell Automation alle Kunden auf, SOFORT zu prüfen, ob ihre Geräte mit dem öffentlichen Internet verbunden sind, und, falls dies der Fall ist, diese Verbindung für Geräte, die nicht speziell für eine öffentliche Internetverbindung ausgelegt sind, dringend zu entfernen.
8	Tuesday, May 14, 2024	Siemens	SSA-592380	In der SIMATIC S7-1500 CPU-Familie und verwand-ten Produkten wurde eine Schwachstelle entdeckt, die es einem Angreifer ermögli-chen könnte, einen Denial-of-Service-Zustand auszulö-sen. Um die Schwachstelle ausnutzen zu können, muss ein Angreifer Zugriff auf die betroffenen Geräte an Port 102/tcp haben.	Alle SEEPEX Steuerungen mit folgender SIEMENS Hardware: SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0)	Derzeit ist keine Lösung geplant
7	Tuesday, February 13, 2024	Siemens	SSA-711309	Denial-of-Service-Schwachstelle in den OPC UA-Implementierungen von SIMATIC-Produkten	Alle SEEPEX-Steuerungen mit folgender SIEMENS Software: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP	Derzeit keine Lösung verfügbar / Update auf die neueste Version
6	Tuesday, December 12, 2023	Siemens	SSA-887801	Informationsweitergabe an LOKALE Angreifer zum Passworder der Zugriffsebene auf SIMATIC S7-1200 und S7-1500 CPUs	Alle SEEPEX Steuerungen mit folgender SIEMENS Hardware: SIMATIC S7-12xx SIMATIC S7-15xx	Ausschluss lokaler Angreifer und/oder TIA Portal Update auf V19 oder höher
5	Tuesday, December 12, 2023	Siemens	SSA-398330	Mehrere Sicherheitslücken auf SIMATIC S7-1500 CPU im GNU/Linux Subsystem	Alle SEEPEX Steuerungen mit folgender SIEMENS Hardware: SIMATIC S7-15xx	Siehe SSA-398330
4	Tuesday, December 12, 2023	Siemens	SSA-592380	Denial-of-Service- Schwachstelle auf SIMATIC S7-1500 CPUs über Port 102/tcp	Alle SEEPEX Steuerungen mit folgender SIEMENS Hardware: SIMATIC S7-15xx	Firmware Update auf V3.1.0 oder höher
3	Saturday, December 9, 2023	Siemens	SSA-711309	Denial-of-Service- Schwachstelle in der OPC UA Implementierung von SIMATIC-Produkten	Alle SEEPEX Steuerungen mit SIEMENS SPSen, die mit einem SEEPEX Gateway (z.B. SPG) verbunden sind	Firmware Update auf V8.1. SP1 oder höher
2	Tuesday, November 14, 2023	Siemens	SSA-699386	Mehrere Sicherheitslücken auf SIEMENS SCALANCE Routern	Alle SEEPEX Schaltschränke mit folgender SIEMENS Hardware: SCALANCE XB-200, XC- 200, XP-200, XF-200BA and XR-300WG	Firmware Update auf V4.5 oder höher
1	Friday, May 28, 2021	Siemens	SSA-434534	Umgehung des Speicherschutzes in den CPU-Familien SIMATIC S7- 1200 und S7-1500	Alle SEEPEX Steuerungen mit folgender SIEMENS Hardware: SIMATIC S7-12xx SIMATIC S7-15xx SIMATIC ET 200SP Open Controller CPU	SIMATIC S7-12xx: Firmware Update auf V4.5 oder höher SIMATIC S7-15xx: Firmware Update auf V2.9.2 oder höher