SSA-711309: Denial of Service Vulnerability in the OPC UA Implementations of SIMATIC Products

Publication Date: 2023-09-12
Last Update: 2024-10-08
Current Version: V2.1
CVSS v3.1 Base Score: 7.5

SUMMARY

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 is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC BRAUMAT: All versions < V8.1 SP1 affected by CVE-2023-28831	Update to V8.1 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109824204/ See further recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions < V2.2 affected by CVE-2023-28831	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822278/ See further recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions < V2.2 affected by CVE-2023-28831	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822278/ See further recommendations from section Workarounds and Mitigations
SIMATIC Comfort/Mobile RT: All versions affected by CVE-2023-28831	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller family:	See below https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations

SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0):	See below https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions >= V3.0.1 < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0):	See below https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions >= V3.0.1 < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants):	See below https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V21.9.7 affected by CVE-2023-28831	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations

SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions >= V30.0.0 < V30.1.0 affected by CVE-2023-28831	Update to V30.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagMonitor: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software:	See below See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions affected by CVE-2023-28831	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V17: All versions < V17 SP1 Update 1 affected by CVE-2023-28831	Update to V17 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109820674/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V18: All versions < V18 Update 1 affected by CVE-2023-28831	Update to V18 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109826242/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.1: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo V4.0: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants):	See below https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DK03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TL03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UL03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DM03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1514SP-2 PN (6ES7514-2DN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UN03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AP03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FP03-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0): All versions < V2.9.7 affected by CVE-2023-28831	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0): All versions < V3.0.3 affected by CVE-2023-28831	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller:	See below https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller V2: All versions < V21.9.7 affected by CVE-2023-28831	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller V3: All versions < V30.1.0 affected by CVE-2023-28831	Update to V30.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V5.0 Update 2 affected by CVE-2023-28831	Update to V5.0 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109823215/ See further recommendations from section Workarounds and Mitigations
SIMATIC SISTAR: All versions < V8.1 SP1 affected by CVE-2023-28831	Update to V8.1 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109824204/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA:	See below https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC OA V3.17: All versions < V3.17 P029 affected by CVE-2023-28831	Update to V3.17 P029 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.18: All versions < V3.18 P019 affected by CVE-2023-28831	Update to V3.18 P019 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.19: All versions < V3.19 P005 affected by CVE-2023-28831	Update to V3.19 P005 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OPC UA Client: All versions < V2.0.0.1 affected by CVE-2023-28831	Update to V2.0.0.1 or later version See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional:	See below See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V16: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V17: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V18: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V19: All versions < V19 Update 2 affected by CVE-2023-28831	Update to V19 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109820999/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Unified OPC UA Server: All versions < V5.0.0.0 affected by CVE-2023-28831	Update to V5.0.0.0 or later version See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7/V8:	See below See recommendations from section Workarounds and Mitigations

SIMATIC WinCC V7.4: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions affected by CVE-2023-28831	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V8.0: All versions < V8.0 Update 5 affected by CVE-2023-28831	Update to V8.0 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109818723/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable the OPC UA feature, if not used

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC BRAUMAT / SISTAR are industry-specific control systems especially for the control and monitoring of recipe-controlled production processes such as in the food, beverages and tobacco industries as well as for comparable batch-oriented production processes.

SIMATIC Cloud Connect 7 is an IoT Gateway to connect programmable logic controllers to cloud services and enables the connection of field devices with OPC UA server Interface as OPC UA clients.

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS 7 and other components.

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 ODK CPUs provide functionality of standard S7-1500 CPUs but additionally provide the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++. They have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Unified OPC UA Client enables WinCC Unified devices to connect with OPC UA servers.

SIMATIC WinCC Unified OPC UA Server allows clients to connect to WinCC Unified via the OPC UA standard.

Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

VULNERABILITY DESCRIPTION

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

Vulnerability CVE-2023-28831

The OPC UA implementations (ANSI C and C++) in affected products contain an integer overflow vulnerability that could cause the application to run into an infinite loop during certificate validation.

This could allow an unauthenticated remote attacker to create a denial of service condition by sending a specially crafted certificate.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-09-12): Publication Date
V1.1 (2023-10-10): Added additional vulnerable products SIMATIC WinCC OA V3.17, SIMATIC WinCC OA V3.18, and SIMATIC WinCC OA V3.19; clarified that both ANSI C and C++ implementations are affected
V1.2 (2023-11-14): Added additional vulnerable products SIMATIC BRAUMAT / SISTAR
V1.3 (2023-12-12): Added SIMATIC Comfort/Mobile RT, SIMATIC IPC DiagMonitor, SIMATIC WinCC Unified OPC UA Client/Server, and SIMATIC PCS neo as affected products; removed unaffected devices: 6ES7513-1RL00-0AB0, 6ES7513-1RM03-0AB0, 6ES7515-2RM00-0AB0, 6ES7515-2RN03-0AB0, 6AG1515-2RM00-7AB0, 6AG2515-2RM00-4AB0, 6ES7517-3HP00-0AB0, 6AG1517-3HP00-4AB0, 6ES7518-4JP00-0AB0, 6AG1518-4JP00-4AB0; added fix for SIMATIC S7-PLCSIM Advanced
V1.4 (2024-01-09): No fix planned for SIMATIC IPC DiagMonitor
V1.5 (2024-02-13): Added fix for SIMATIC WinCC Unified OPC UA Client/Server; Added SIMATIC PCS 7 V9.1 as affected; Added specific mitigation measure for CVE-2023-28831 (disable OPC UA)
V1.6 (2024-03-12): Removed unaffected device SIMATIC S7-1200 CPU family (incl. SIPLUS variants), added SIMATIC WinCC (Classic and Runtime Professional) and Totally Integrated Automation Portal to the list of affected devices, no fix planned for SIMATIC PCS 7 V9.1
V1.7 (2024-04-09): Added SIMATIC NET PC Software as affected product; added fix for SIMATIC NET PC Software V17, V18; added fix for SIMATIC S7-1500 Software Controller V3; removed unaffected product TIA Portal
V1.8 (2024-05-14): Added fix for SIMATIC ET 200SP Open Controller CPU 1515SP PC2 V30
V1.9 (2024-06-11): Added fix for SIMATIC WinCC Runtime Professional V19
V2.0 (2024-07-09): Added fix for SIMATIC WinCC V8.0
V2.1 (2024-10-08): No fix planned for SIMATIC PCS neo V4.0; removed SIMATIC PCS neo V4.1 as not affected

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.