SSA-711309: Denial of Service Vulnerability in the ANSI C OPC UA SDK of SIMATIC Products

Publication Date: 2023-09-12
Last Update: 2023-09-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

The ANSI C OPC UA implementation as used in several SIMATIC products contains 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 updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822278/
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109822278/
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions >= V3.0.1 < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions >= V3.0.1 < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V21.9.7	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109759122/

SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions >= V30.0.0	Currently no fix is available
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SK03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DK03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TL03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UL03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SM03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DM03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RM03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1514SP F-2 PN (6ES7514-2SN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1514SP-2 PN (6ES7514-2DN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1514SPT F-2 PN (6ES7514-2WN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1514SPT-2 PN (6ES7514-2VN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UN03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AP03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FP03-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 Software Controller V2: All versions < V21.9.7	Update to V21.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/
SIMATIC S7-1500 Software Controller V3: All versions	Currently no fix is available
SIMATIC S7-PLCSIM Advanced: All versions	Currently no fix is available
SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515R-2 PN (6AG1515-2RM00-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1515R-2 PN TX RAIL (6AG2515-2RM00-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0): All versions < V2.9.7	Update to V2.9.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1517H-3 PN (6AG1517-3HP00-4AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIPLUS S7-1500 CPU 1518HF-4 PN (6AG1518-4JP00-4AB0): All versions < V3.0.3	Update to V3.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

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

PRODUCT DESCRIPTION

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 S7-1200 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 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-28831

The ANSI C OPC UA SDK contains 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

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.