SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices

Publication Date:	2023-01-10
Last Update:	2023-01-10
Current Version:	V1.0
CVSS v3.1 Base Score:	4.6

SUMMARY

Affected models of the S7-1500 CPU product family do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device can not be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code.

As exploiting this vulnerability requires physical tampering with the product, Siemens recommends to assess the risk of physical access to the device in the target deployment and to implement measures to make sure that only trusted personnel have access to the physical hardware.

The vulnerability is related to the hardware of the product. Siemens has released new hardware versions for several CPU types of the S7-1500 product family in which this vulnerability is fixed and is working on new hardware versions for remaining PLC types to address this vulnerability completely. See the chapter “Additional Information” below for more details.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AK02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511C-1 PN (6ES7511-1CK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FK02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511T-1 PN (6ES7511-1TK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1511TF-1 PN (6ES7511-1UK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512C-1 PN (6ES7512-1CK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4F PN/DP (6ES7518-4FP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515R-2 PN (6AG1515-2RM00-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1515R-2 PN TX RAIL (6AG2515-2RM00-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN00-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1517H-3 PN (6AG1517-3HP00-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0): All versions	Currently no fix is planned See 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:

- Restrict physical access to affected devices to trusted personnel to avoid hardware tampering (e.g., place the devices in locked control cabinets)

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 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 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.

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the STEP 7 program if required.

The 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.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2022-38773

Affected devices do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device can not be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code.

CVSS v3.1 Base Score	4.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:T/RC:C
CWE	CWE-1326: Missing Immutable Root of Trust in Hardware

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Yuanzhe Wu and Ang Cui from Red Balloon Security for coordinated disclosure

ADDITIONAL INFORMATION

Siemens has released the following new hardware versions of the S7-1500 product family. They contain a new secure boot mechanism that resolves the vulnerability:

- SIMATIC S7-1500 CPU 1511-1 PN (6ES7511-1AL03-0AB0)
- SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AM03-0AB0)
- SIMATIC S7-1500 CPU 1511F-1 PN (6ES7511-1FL03-0AB0)
- SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FM03-0AB0)
- SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RM03-0AB0)
- SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RN03-0AB0)

Siemens is working on new hardware versions for additional PLC types to address this vulnerability further.

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 (2023-01-10):	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.