SSA-686531: Hardware based manufacturing access on S7-1200 and S7-200 SMART

Publication Date: 2019-11-12
Last Update: 2020-07-14
Current Version: V1.2
CVSS v3.1 Base Score: 6.8

SUMMARY

There is an access mode used during manufacturing of SIMATIC S7-1200 and S7-200 SMART CPUs that allows additional diagnostic functionality. Using this functionality requires physical access to the CPU during boot process.

If additional protection from unauthorized use is needed Siemens provides specific countermeasures via an update of the device boot loader.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family V4.x (incl. SIPLUS variants): All versions with Function State (FS) < 11	Update to version >= V4.4.1 and Function State (FS) >= 11
SIMATIC S7-1200 CPU family < V4.x (incl. SIPLUS variants): All versions	Firmware versions less than V4.x cannot be updated. For remediation see the recommendations from section “Workarounds and Mitigations”.
SIMATIC S7-200 SMART CPU ST20 (6ES7 288-1ST20-0AA0): All versions <= V2.5.0 and Function State (FS) <= 9	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU ST30 (6ES7 288-1ST30-0AA0): All versions <= V2.5.0 and Function State (FS) <= 9	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU ST40 (6ES7 288-1ST40-0AA0): All versions <= V2.5.0 and Function State (FS) <= 8	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU ST60 (6ES7 288-1ST60-0AA0): All versions <= V2.5.0 and Function State (FS) <= 8	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU SR20 (6ES7 288-1SR20-0AA0): All versions <= V2.5.0 and Function State (FS) <= 11	Update to version >= V2.5.1 and the latest boot loader version

SIMATIC S7-200 SMART CPU SR30 (6ES7 288-1SR30-0AA0): All versions <= V2.5.0 and Function State (FS) <= 10	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU SR40 (6ES7 288-1SR40-0AA0): All versions <= V2.5.0 and Function State (FS) <= 10	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU SR60 (6ES7 288-1SR60-0AA0): All versions <= V2.5.0 and Function State (FS) <= 12	Update to version >= V2.5.1 and the latest boot loader version
SIMATIC S7-200 SMART CPU CR40 (6ES7 288-1CR40-0AA0): All versions <= V2.2.2 and Function State (FS) <= 8	Update to version >= V2.2.3 and the latest boot loader version
SIMATIC S7-200 SMART CPU CR60 (6ES7 288-1CR60-0AA0): All versions <= V2.2.2 and Function State (FS) <= 10	Update to version >= V2.2.3 and the latest boot loader version
SIMATIC S7-200 SMART CPU CR20s (6ES7 288-1CR20-0AA1): All versions <= V2.3.0 and Function State (FS) <= 3	Update to version >= V2.3.0 and the latest boot loader version Note that the firmware version currently remains at V2.3.0, only the boot loader is updated.
SIMATIC S7-200 SMART CPU CR30s (6ES7 288-1CR30-0AA1): All versions <= V2.3.0 and Function State (FS) <= 3	Update to version >= V2.3.0 and the latest boot loader version Note that the firmware version currently remains at V2.3.0, only the boot loader is updated.
SIMATIC S7-200 SMART CPU CR40s (6ES7 288-1CR40-0AA1): All versions <= V2.3.0 and Function State (FS) <= 3	Update to version >= V2.3.0 and the latest boot loader version Note that the firmware version currently remains at V2.3.0, only the boot loader is updated.
SIMATIC S7-200 SMART CPU CR60s (6ES7 288-1CR60-0AA1): All versions <= V2.3.0 and Function State (FS) <= 3	Update to version >= V2.3.0 and the latest boot loader version Note that the firmware version currently remains at V2.3.0, only the boot loader is updated.

WORKAROUNDS AND MITIGATIONS

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

- Ensure physical access protection
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

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

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

The S7-200 SMART series is a line of micro-programmable logic controllers that can control a variety of small automation applications.

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-2019-13945

There is an access mode used during manufacturing of the affected devices that allows additional diagnostic functionality.

The security vulnerability could be exploited by an attacker with physical access to the UART interface during boot process.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-749: Exposed Dangerous Method or Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ali Abbasi from Ruhr University of Bochum for coordinated disclosure
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-11-12):	Publication Date
V1.1 (2019-12-10):	Added SIMATIC S7-200 SMART to the list of affected devices. SIPLUS devices now explicitly mentioned in the list of affected products
V1.2 (2020-07-14):	Added solution information for SIMATIC S7-1200 and SIMATIC S7-200 SMART

TERMS OF USE