SSA-686531: Hardware based manufacturing access on S7-1200

Publication Date: 2019-11-12
Last Update: 2019-11-12
Current Version: V1.0
CVSS v3.1 Base Score: 6.8

SUMMARY

There is an access mode used during manufacturing of S7-1200 CPUs that allows additional diagnostic functionality. Using this functionality requires physical access to the UART interface during boot process.

Siemens is working on a solution and recommends specific countermeasures until the solution is available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
S7-1200 CPU: All versions	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:

- 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.

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 S7-1200 CPUs that allows additional diagnostic functionality.

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

At the time of advisory publication no public exploitation of this security vulnerability was known.

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

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

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.