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

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 UART interface during boot process.

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

AFFECTED PRODUCTS AND SOLUTION

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions</td>
<td>See recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>SIMATIC S7-200 SMART CPU family: All versions</td>
<td>See recommendations from section Workarounds and Mitigations</td>
</tr>
</tbody>
</table>

WORKAROUNDS AND MITIGATIONS

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

- Ensure physical access protection

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 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.

<table>
<thead>
<tr>
<th>CVSS v3.1 Base Score</th>
<th>6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE</td>
<td>CWE-749: Exposed Dangerous Method or Function</td>
</tr>
</tbody>
</table>

**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
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.