SSA-617264: Multiple Security Vulnerabilities in SIMATIC S7-400 V5 PN CPUs

Publication Date: 2012-07-30
Last Update: 2020-04-13
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

When receiving malformed network data, SIMATIC S7-400 V5 PN CPUs may go into defect mode. This would allow attackers to perform a Denial-of-Service attack on the CPUs.

Siemens will not publish a fix for this vulnerability as this product version is discontinued since October 2011 [1]. Version V6 is not affected by these specific problems. [1] https://support.industry.siemens.com/cs/ww/en/view/50252551

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 CPU 414-3 PN/DP (6ES7414-3EM05-0AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-3 PN/DP (6ES7416-3ER05-0AB0, incl. SIPLUS variant): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-3 PN/DP (6ES7416-3FR05-0AB0): 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:

- Access to the production network in which the devices are deployed must be controlled and minimized as much as possible.

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 in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

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-2012-3017

A Denial-of-Service can be caused via malformed HTTP communication or malformed IP packets.

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:U/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts
- 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 (2012-07-30):	Publication Date
V1.1 (2020-04-13):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE

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.