SSA-763427: Vulnerability in Communication Processor (CP) modules SIMATIC CP 343-1, TIM 3V-IE, TIM 4R-IE, and CP 443-1

Publication Date	2015-11-27
Last Update	2016-04-29
Current Version	V1.3
CVSS Overall Score	7.6

SUMMARY

Siemens has released updates for Communication Processor (CP) module families SIMATIC CP 343-1/TIM 3V-IE/TIM 4R-IE/CP 443-1 to resolve an authentication bypass vulnerability that could allow unauthenticated users to perform administrative operations under certain conditions.

AFFECTED PRODUCTS

- SIMATIC CP 343-1 Advanced: All firmware versions < V3.0.44
- SIMATIC CP 343-1 Lean / CP 343-1: All firmware versions < V3.1.1
- SIMATIC TIM 3V-IE / TIM 3V-IE Advanced: All firmware versions < V2.6.0
- SIMATIC TIM 3V-IE DNP3: All firmware versions < V3.1.0
- SIMATIC TIM 4R-IE: All firmware versions < V2.6.0
- SIMATIC TIM 4R-IE DNP3: All firmware versions < V3.1.0
- SIMATIC CP 443-1 / CP 443-1 Advanced: All firmware versions < V3.2.9

DESCRIPTION

Communication processor (CP) modules SIMATIC CP 343-1/TIM 3V-IE/TIM 4R-IE/CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet or Telecontrol communication.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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.

Vulnerability Description (CVE-2015-8214)

The implemented access protection level enforcement of the affected communication processors (CP) could possibly allow unauthenticated users to perform administrative operations on the CPs if network access (port 102/TCP) is available and the CPs' configuration was stored on their corresponding CPUs.

CVSS Base Score	9.7
CVSS Temporal Score	7.6
CVSS Overall Score	7.6 (AV:N/AC:L/Au:N/C:P/I:C/A:C/E:POC/RL:OF/RC:C)

Mitigating Factors

The attacker must have

- network access to the affected devices,
- configuration data for the CP must be stored on CPU, and
- Firewall functionality of Advanced-CPs must be turned off for port 102/TCP.

SOLUTION

Siemens provides firmware updates for the following products which fix the vulnerability and recommends customers to update to the new fixed versions:

- SIMATIC CP 343-1 Advanced: Update firmware to V3.0.44 [1]
- SIMATIC CP 343-1 Lean / CP 343-1: Update firmware to V3.1.1 [2]
- SIMATIC TIM 3V-IE / TIM 3V-IE Advanced: Update firmware to V2.6.0 [3]
- SIMATIC TIM 3V-IE DNP3: Update firmware to V3.1.0 [4]
- SIMATIC TIM 4R-IE: Update firmware to V2.6.0 [3]
- SIMATIC TIM 4R-IE DNP3: Update firmware to V3.1.0 [5]
- SIMATIC CP 443-1: Update firmware to V3.2.9 [6]
- SIMATIC CP 443-1 Advanced: Update firmware to V3.2.9 [7]

Siemens recommends customers to generally apply the following mitigations, especially until patches can be applied:

- Activate firewall functionality on Advanced-CPs and reject S7-communication at the perimeter port
- Apply cell protection concept [8]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [9]

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Lei ChengLin (Z-0ne) from Fengtai Technologies' Security Research Team for coordinated disclosure of the vulnerability
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts.

ADDITIONAL RESOURCES

[1] Firmware update V3.0.44 for SIMATIC CP 343-1 Advanced modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109480765

[2] Firmware update V3.1.1 for SIMATIC CP 343-1 Lean / CP 343-1 can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109486101

[3] Firmware update V2.6.0 for SIMATIC TIM 3V-IE / TIM 3V-IE Advanced and TIM 4R-IE modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109481769

[4] Firmware update V3.1.0 for SIMATIC TIM 3V-IE DNP3 modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109481766

[5] Firmware update V3.1.0 for SIMATIC TIM 4R-IE DNP3 modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109481765

[6] Firmware update V3.2.9 for SIMATIC CP 443-1 modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109482246

[7] Firmware update V3.2.9 for SIMATIC CP 443-1 Advanced modules can be obtained for free from:
https://support.industry.siemens.com/cs/ww/en/view/109482247

[8] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[9] Further information about Defense-in-Depth:
http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx

[10] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[11] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2015-11-27): Publication Date
V1.1 (2016-01-29): Added fix information for SIMATIC TIM 3V-IE and TIM 4R-IE modules
V1.2 (2016-02-01): Added fix information for SIMATIC CP 443-1 / CP 443-1 Advanced
V1.3 (2016-04-29): Added fix information for SIMATIC CP343-1 Lean / CP 343-1

DISCLAIMER