SSA-275839: Denial-of-Service Vulnerability in Industrial Products

Publication Date: 2017-05-08
Last Update: 2019-02-12
Current Version: V2.1
CVSS v3.0 Base Score: 6.5

SUMMARY

Several industrial products are affected by a vulnerability that could allow an attacker to cause a Denial-of-Service condition via PROFINET DCP network packets under certain circumstances. Precondition for this scenario is a direct Layer 2 access to the affected products.

Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

On a single host the affected component is shared among the affected products. Installing one fixed version will mitigate the vulnerability for all Siemens applications installed on the single host.

Affected Product and Versions	Remediation
Primary Setup Tool (PST): All versions < V4.2 HF1	Update to V4.2 HF1 https://support.industry.siemens.com/cs/ww/en/view/19440762
SIMATIC Automation Tool: All versions < V3.0	Update to V3.0 https://support.industry.siemens.com/cs/ww/en/view/98161300
SIMATIC NET PC-Software: All versions < V14 SP1	Upgrade to V14 SP1 https://support.industry.siemens.com/cs/ww/en/view/109747482
SIMATIC PCS 7 V8.1 and earlier versions: All versions	See recommendations from section Workarounds and Mitigations, or upgrade to V9.0 https://www.siemens.de/automation/partner
SIMATIC PCS 7 V8.2: All versions < V8.2 SP1	Update to V8.2 SP1 To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support.
SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2	Update to V13 SP 2 https://support.industry.siemens.com/cs/ww/en/view/109745155
SIMATIC STEP 7 (TIA Portal) V14: All versions < V14 SP1	Update to V14 SP 1 https://support.industry.siemens.com/cs/ww/en/view/109745984
SIMATIC STEP 7 V5.X: All versions < V5.6	Update to V5.6 https://support.industry.siemens.com/cs/ww/en/view/109747706
SIMATIC WinAC RTX 2010 SP2: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC WinAC RTX F 2010 SP2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V13: All versions < V13 SP2	Update to V13 SP2 https://support.industry.siemens.com/cs/ww/en/view/109746073
SIMATIC WinCC (TIA Portal) V14: All versions < V14 SP1	Update to V14 SP 1 https://support.industry.siemens.com/cs/ww/en/view/109745460
SIMATIC WinCC V7.2 and prior: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions < V7.3 Update 15	Update to V7.3 Update 15 https://support.industry.siemens.com/cs/ww/en/view/109750182
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Upd1	Update to V7.4 SP1 Upd1 https://support.industry.siemens.com/cs/ww/en/view/109748024
SIMATIC WinCC flexible 2008: All versions < flexible 2008 SP5	Upgrade to WinCC flexible 2008 SP5 https://support.industry.siemens.com/cs/ww/en/view/109749111
SINAUT ST7CC: All versions installed in conjunction with SIMATIC WinCC < V7.3 Update 15	Update SIMATIC WinCC to V7.3 Update 15 or newer https://support.industry.siemens.com/cs/ww/en/view/109750182
SINEMA Server: All versions < V14	Upgrade to V14 https://support.industry.siemens.com/cs/ww/en/view/109748854
SINUMERIK 808D Programming Tool: All versions < V4.7 SP4 HF2	Update to V4.7 SP4 HF2 SINUMERIK software can be obtained from your local Siemens account manager
SMART PC Access: All versions < V2.3	Update to V2.3 SMART PC Access V2.3 can be obtained by contacting your local Siemens representative or customer support: https://w3.siemens.com/aspa_app/
STEP 7 - Micro/WIN SMART: All versions < V2.3	Update to V2.3 Micro/WIN SMART V2.3 can be obtained by contacting your local Siemens representative or customer support: https://w3.siemens.com/aspa_app/
Security Configuration Tool (SCT): All versions < V5.0	Update to V5.0 https://support.industry.siemens.com/cs/de/en/view/109747539

WORKAROUNDS AND MITIGATIONS

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

- Apply cell protection concept
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth

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

SIMATIC WinCC (TIA Portal) is an engineering software to configure and program SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs running WinCC Runtime Advanced or SCADA System WinCC Runtime Professional visualization software.

SIMATIC STEP 7 V5.X and STEP 7 (TIA Portal) are engineering software for SIMATIC PLC products.

STEP 7- Micro/WIN SMART is the programming software for the S7-200 SMART CPU.

SMART PC Access is an OPC DA test tool for use with S7-200 SMART CPU.

SIMATIC Automation Tool allows commissioning, adjusting and service in combination with S7-1200 and S7-1500 Controllers without engineering framework.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

The Primary Setup Tool (PST) allows initial network configuration of SIMATIC NET Industrial Ethernet products.

The Security Configuration Tool (SCT) is an engineering software for security devices such as SCALANCE-S or CP 443-1 Advanced.

SINEMA Server is a network management software designed by Siemens for use in Industrial Ethernet networks.

SINAUT ST7CC allows remote monitoring and control of plants.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

The SINUMERIK 808D Programming Tool is the PLC engineering for SINUMERIK 808D.

SIMATIC WinCC flexible panels and runtime systems are used for process visualization and control operations.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2017-6865

Specially crafted PROFINET DCP broadcast packets sent to the affected products on alocal Ethernet segment (Layer 2) could cause a Denial-of-Service condition of someservices. The services require manual restart to recover.

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Duan JinTong, Ma ShaoShuai, and Cheng Lei from NSFOCUS Security Team for coordinated disclosure of vulnerability.
- CNCERT/CC for coordination efforts.

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 (2017-05-08):	Publication Date
V1.1 (2017-06-07):	Added update information for STEP 7 V5.X, SIMATIC WinCC, and SCT
V1.2 (2017-06-20):	Added update information for Primary Setup Tool
V1.3 (2017-07-06):	Added upgrade information for PCS 7
V1.4 (2017-07-21):	Added upgrade information for SINEMA Server
V1.5 (2017-08-16):	Added update information for STEP 7 - Micro/WIN SMART, SIMATIC Automation Tool, and SINUMERIK 808D Programming Tool
V1.6 (2017-10-09):	Added update information for WinCC V7.3
V1.7 (2017-11-09):	Added update information for SIMATIC NET PC-Software
V1.8 (2018-01-18):	New advisory format, fixed version information and added update information for SMART PC Access
V1.9 (2018-02-22):	Added fix information for WinCC flexible 2008
V2.0 (2018-06-12):	Detailed PCS 7 affection; Added update information for PCS V8.2
V2.1 (2019-02-12):	Added update information for SINAUT ST7CC

TERMS OF USE