

SSA-841348: Multiple Vulnerabilities in the UMC Stack

Publication Date: 2020-07-14
 Last Update: 2020-09-08
 Current Version: V1.2
 CVSS v3.1 Base Score: 6.7

SUMMARY

The latest update for the below listed products fixes two security vulnerabilities that could allow an attacker to cause a partial Denial-of-Service on the UMC component of the affected devices under certain circumstances, and one vulnerability that could allow an attacker to locally escalate privileges from a user with administrative privileges to execute code with SYSTEM level privileges.

Siemens has released updates for several affected products and recommends that customers update to the latest version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Opcenter Execution Discrete: All versions < V3.2	Update to V3.2 or later version https://support.sw.siemens.com/
Opcenter Execution Foundation: All versions < V3.2	Update to V3.2 or later version https://support.sw.siemens.com/
Opcenter Execution Process: All versions < V3.2	Update to V3.2 or later version https://support.sw.siemens.com/
Opcenter Intelligence: All versions	See recommendations from section Workarounds and Mitigations
Opcenter Quality: All versions < V11.3	Update to V11.3 or later version https://support.sw.siemens.com/
Opcenter RD&L: V8.0	Update to V8.1 or later version https://support.sw.siemens.com/
SIMATIC IT LMS: All versions only affected by CVE-2020-7587, CVE-2020-7588	See recommendations from section Workarounds and Mitigations
SIMATIC IT Production Suite: All versions only affected by CVE-2020-7587, CVE-2020-7588	See recommendations from section Workarounds and Mitigations
SIMATIC Notifier Server for Windows: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC PCS neo: All versions < V3.0 SP1	Update to V3.0 SP1 To obtain SIMATIC PCS neo V3.0 SP1 contact your local support.
SIMATIC STEP 7 (TIA Portal) V15: All versions < V15.1 Update 5	Update to V15.1 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC STEP 7 (TIA Portal) V16: All versions < V16 Update 2	Update to V16 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861
SIMOCODE ES: All versions	See recommendations from section Workarounds and Mitigations
Soft Starter ES: 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:

- Have the software running on systems within trusted networks
- For CVE-2020-7581 make sure that there is no executable at the following locations:
 - *C:\Program.exe,*
 - *C:\Program Files\Common.exe, or*
 - *C:\Program Files\Common Files\Siemens\Automation\Simatic.exe*

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 Notifier monitors data and sends notifications based on configured events for access from anywhere.

SIMOCODE ES is the central software package for the configuration, commissioning, operation, and diagnosis of SIMOCODE pro.

Soft Starter ES is the central software for configuration, commissioning, operation and diagnostics of the SIRIUS 3RW55, 3RW52 and 3RW44 soft starters.

SIMATIC PCS neo is a distributed control system (DCS).

The Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

SIMATIC IT Unified Architecture Foundation (SIT UAF) is a framework to build and run state-of-the-art manufacturing operations management (MOM) applications.

Opcenter Execution Discrete (formerly known as “SIMATIC IT Unified Architecture Discrete Manufacturing”) is a specialized Manufacturing Execution System addressing the needs of the discrete industry market, focusing on job-shop part manufacturing and complex manual assembly.

Opcenter Execution Process (formerly known as “SIMATIC IT Unified Architecture Process Industries”) is Siemens’ MES system for the CPG and Process industries. Based on the latest technology, it enables to implement the strategy for the complete digitalization of manufacturing.

Opcenter RD&L (formerly known as “SIMATIC IT R&D Suite”) offers companies in CPG and process industries a scalable and flexible platform to streamline, optimize, and align all formulated product data management.

Opcenter Quality is a quality management system (QMS) that enables organizations to safeguard compliance, optimize quality, reduce defect and rework costs and achieve operational excellence by increasing process stability. The integrated process capabilities (control charts, statistics, quality gates) can detect production errors to avoid further processing and shipment of nonconforming material.

Opcenter Intelligence (formerly known as “Manufacturing Intelligence”) connects, organizes and aggregates manufacturing data from disparate company sources into cohesive, intelligent and contextualized information.

SIMATIC IT Line Monitoring System is designed to monitor plant floor performance, blending real-time and transactional systems, for a line visibility & control. This line-monitoring capability allows manufacturers to increase production efficiency, as well as optimize performance, use reporting to their best advantage, and reduce line inefficiencies, while incrementing product yields. Line Monitoring System within SIMATIC IT allows for automatic and real-time collection of production relevant data directly from the factory floor.

SIMATIC IT Production Suite is a plant-centric IT solution building the link between Business Systems (e.g. ERP) and Control Systems.

User Management Component (UMC) is an integrating component that enables system-wide, central maintenance of users.

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-2020-7581

A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-428: Unquoted Search Path or Element

Vulnerability CVE-2020-7587

Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself.

On some cases the vulnerability could leak random information from the remote service.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2020-7588

Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Victor Fidalgo from INCIBE for coordinated disclosure of CVE-2020-7581
- Reid Wightman from Dragos for coordinated disclosure of CVE-2020-7581 and CVE-2020-7587

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 (2020-07-14):	Publication Date
V1.1 (2020-08-11):	Added solution for SIMATIC PCS neo
V1.2 (2020-09-08):	Added solution for SIMATIC STEP 7 (TIA Portal) V15

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.