SSA-886615: Vulnerability in SIMATIC IT Production Suite

Publication Date: 2018-11-13
Last Update: 2018-11-13
Current Version: V1.0
CVSS v3.0 Base Score: 7.7

SUMMARY

The latest update for SIMATIC IT Production Suite fixes a vulnerability that could allow authorized users with knowledge of a valid user name and physical or network access to the affected system to bypass the application-level authentication.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC IT LMS: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IT Production Suite: Versions V7.1 < V7.1 Upd3	Update to V7.1 Upd3. Contact Product Support to obtain the update. https://www.plm.automation.siemens.com/global/en/support/
SIMATIC IT UA Discrete Manufacturing: Versions < V1.2	See recommendations from section Workarounds and Mitigations
SIMATIC IT UA Discrete Manufacturing: Versions V1.2	Update the contained components SIMATIC IT Administrative Tools, SIMATIC IT Basic Service, and SIMATIC IT Full Services to V7.1 Upd3 (or later). Contact Product Support to obtain the update. https://www.plm.automation.siemens.com/global/en/support/
SIMATIC IT UA Discrete Manufacturing: Versions V1.3	Update the contained components SIMATIC IT Administrative Tools, SIMATIC IT Basic Service, and SIMATIC IT Full Services to V7.1 Upd3 (or later). Contact Product Support to obtain the update. https://www.plm.automation.siemens.com/global/en/support/
SIMATIC IT UA Discrete Manufacturing: Versions V2.3	Update the contained components SIMATIC IT Administrative Tools, SIMATIC IT Basic Service, and SIMATIC IT Full Services to V7.1 Upd3 (or later). Contact Product Support to obtain the update. https://www.plm.automation.siemens.com/global/en/support/

SIMATIC IT UA Discrete Manufacturing: Versions V2.4	The latest V2.4 release containing SIMATIC IT Administrative Tools, SIMATIC IT Basic Service, and SIMATIC IT Full Services V7.1 Upd3 is available from GTAC Download. https://download.industrysoftware.automation.siemens.com/

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to affected installations.

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

SIMATIC IT Unified Architecture Discrete Manufacturing is designed to satisfy the most common needs of industries with a hierarchical structure in which specific macro-areas are dedicated to executing discrete manufacturing functionalities in various stages in order to produce the desired product. SIMATIC IT UADM provides you with all basic functionalities for:

- Modelling your production environment, consisting in locations, machines required for production, work operations, tools, materials, etc.
- Defining how products are produced (that is, defining the various operations and/or steps involved in their production).
- Creating production orders, in which you define the type of production to be adopted and the quantity to be produced for the order you have in mind.
- Scheduling production according to your needs.
- Tracking and monitoring production, to see how the execution of your work order is progressing.

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.

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-2018-13804

An attacker with network access to the installation could bypass the application-level authentication.

In order to exploit the vulnerability, an attacker must obtain network access to an affected installation and must obtain a valid username to the system.

Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	7.7
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C

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 (2018-11-13): Publication Date

TERMS OF USE