SSA-984700: Password Storage Vulnerability in SIMATIC IT UADM

Publication Date: 2019-10-08
Last Update: 2019-10-08
Current Version: V1.0
CVSS v3.0 Base Score: 6.8

SUMMARY

A vulnerability has been identified in the SIMATIC IT Unified Architecture Discrete Manufacturing product that caused a password to be encrypted with a predicable encryption key. An authenticated attacker could potentially recover the password and gain access to the TeamCenter station connected to the instance.

Siemens provides updates to address the vulnerability, and recommends specific mitigations.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC IT UADM: All versions < V1.3	Update to V1.3 SIMATIC IT UADM software can be obtained from your local Siemens account manager.

WORKAROUNDS AND MITIGATIONS

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

- Protect network access to port 1434/tcp of machines running SIMATIC IT UADM software.
- Apply cell protection concept and implement 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 IT Unified Architecture Discrete Manufacturing (SIMATIC IT UADM) is a software product specifically designed and developed by Siemens by leveraging the SIMATIC IT Unified Architecture foundation. SIMATIC IT UADM is the specialized product addressing the needs of the discrete industry market. It is designed to satisfy the most common needs of industries in which specific macro areas are dedicated to executing sequential discrete manufacturing functions in order to produce the desired product.

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-2019-13929

An authenticated remote attacker with network access to port 1434/tcp of SIMATIC IT UADM could potentially recover a password that can be used to gain read and write access to the related TeamCenter station.

The security vulnerability could be exploited only if the attacker is authenticated. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system.

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

CVSS v3.0 Base Score	6.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/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 (2019-10-08):	Publication Date

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.