SSA-649853: Improper Certificate Validation Vulnerability in Industrial Edge Management

Publication Date: 2022-10-11
Last Update: 2022-10-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

Industrial Edge Management contains a vulnerability that could allow an unauthenticated attacker to spoof a trusted entity by interfering in the communication path between the Industrial Edge Management (IEM) and the Industrial Edge Hub (IEH) using a crafted certificate.

An attacker could use this to inject malicious maintenance requests (e.g. sending statistics, activating remote support, exchanging the initial keys when onboarding, querying new extensions).

Siemens has released an update for the Industrial Edge Management and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Industrial Edge Management: All versions < V1.5.1	Update to V1.5.1 or later version https://iehub.eu1.edge.siemens.cloud/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

Industrial Edge Management (IEM) enables a centralized management of Siemens Industrial Edge Devices and Edge Applications. IEM is tailored to customer's needs and is operated by the customer (on-premises).

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-2022-40147

The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

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 (2022-10-11): 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.