SSA-692317: Authorization Bypass Vulnerability in Industrial Edge

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for Industrial Edge fixes a vulnerability that could allow an unauthenticated attacker to change the password of any user in the system. With this an attacker could impersonate any valid user on an affected system.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Industrial Edge Management: All versions < V1.3	Update to V1.3 or later version https://iehub.eu1.edge.siemens.cloud/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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

The 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).

App Management:

- Remote configuration and deployment of programmed Edge Apps & System Services on edge devices
- Remote starting, stopping and monitoring of installed Edge apps on devices

Device Management:

- Remote system diagnosis of Edge devices

* Remote deployment of security/firmware updates for Edge Devices

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-2021-37184

An unauthenticated attacker could change the the password of any user in the system under certain circumstances. With this an attacker could impersonate any valid user on an affected system.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-639: Authorization Bypass Through User-Controlled Key

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 (2021-09-14): 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.