

Forum:[Hack Forums](#)

Thread: [Siemens Building X - Security Manager Edge Controller](#)

Stanley - December 27, 2025, 10:55 pm

Siemens Building X - Security Manager Edge Controller

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory. For the most up-to-date information on vulnerabilities in this advisory, please see Siemens' ProductCERT Security Advisories (CERT Services | Services | Siemens Global).

View CSAF

1. EXECUTIVE SUMMARY

CVSS v4 5.9

ATTENTION: Low attack complexity

Vendor: Siemens

Equipment: Building X - Security Manager Edge Controller (ACC-AP)

Vulnerability: Improper Verification of Cryptographic Signature

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to upload maliciously modified firmware onto the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Siemens reports the following products are affected:

Building X - Security Manager Edge Controller (ACC-AP): All versions

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

Affected devices do not properly check the integrity of firmware updates. This could allow a local attacker to upload maliciously modified firmware onto the device. In a second scenario, a remote attacker who is able to intercept the transfer of valid firmware from the server to the device could modify the firmware "on the fly".

CVE-2022-31807 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.2 has been calculated; the CVSS vector string is (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).

A CVSS v4 score has also been calculated for CVE-2022-31807. A base score of 5.9 has been calculated; the CVSS vector string is

(CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER

Siemens ProductCERT reported this vulnerability to CISA.

4. MITIGATIONS

Siemens has identified the following specific workarounds and mitigations users can apply to

reduce risk:

Building X - Security Manager Edge Controller (ACC-AP): Use the ACC Firmware App to apply updates in a controlled and authenticated manner, ensuring that only verified firmware packages from the official SIOS portal are installed on the controller. Validate the integrity of the downloaded firmware by confirming its hash value. Access to the controller should remain limited to authorized personnel, and credentials must be protected and updated according to policy to reduce the risk of unauthorized modifications or the installation of tampered firmware

Building X - Security Manager Edge Controller (ACC-AP): Currently no fix is planned

As a general security measure, Siemens recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for industrial security and following recommendations in the product manuals.

Additional information on industrial security by Siemens can be found on the Siemens industrial security webpage

For more information see the associated Siemens security advisory SSA-420375 in HTML and CSAF.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs). Recognize VPNs may have vulnerabilities, should be updated to the most recent version available, and are only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time. This vulnerability is not exploitable remotely.

5. UPDATE HISTORY

December 11, 2025: Initial Republication of Siemens Product CERT SSA-420375

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-07>

cleari - December 27, 2025, 10:59 pm

ow, i need o plus w for fulfil lment tty.. Ow/