Forum:Hack Forums

Thread: Siemens Gridscale X Prepay

Stanley - *December 26, 2025, 4:35 pm*

Siemens Gridscale X Prepay

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 6.9
ATTENTION: Exploitable remotely/low attack complexity
Vendor: Siemens
Equipment: Gridscale X Prepay
Vulnerabilities: Observable Response Discrepancy, Authentication Bypass by Capture-replay

2. RISK EVALUATION
Successful exploitation of these vulnerabilities could allow an attacker to enumerate valid user names and to bypass locked-out user sessions.
3. TECHNICAL DETAILS
3.1 AFFECTED PRODUCTS
Siemens reports that the following product is affected:

Gridscale X Prepay: Version prior to 4.2.1

3.2 VULNERABILITY OVERVIEW
3.2.1 OBSERVABLE RESPONSE DISCREPANCY CWE-204
The affected application is vulnerable to user enumeration due to distinguishable responses. This could allow an unauthenticated remote attacker to determine if a user is valid or not, enabling a brute force attack with valid users.
CVE-2025-40806 has been assigned to this vulnerability. A CVSS v3.1 base score of 5.3 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
A CVSS v4 score has also been calculated for CVE-2025-40806. A base score of 6.9 has been calculated; the CVSS vector string is (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N).
3.2.2 AUTHENTICATION BYPASS BY CAPTURE-REPLAY CWE-294
The affected application is vulnerable to capture-replay of authentication tokens. This could allow an authenticated but already locked-out user to establish still valid user sessions.
CVE-2025-40807 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.3 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
A CVSS v4 score has also been calculated for CVE-2025-40807. A base score of 5.3 has been calculated; the CVSS vector string is (CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N).
3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Energy

COUNTRIES/AREAS DEPLOYED: Worldwide
COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER
Kira from The Raven Security reported these vulnerabilities to Siemens ProductCERT.Siemens ProductCERT reported these vulnerabilities to CISA.
4. MITIGATIONS
Siemens has identified the following specific workarounds and mitigations users can apply to reduce risk:

Gridscale X Prepay: Please contact your local Siemens representative for further information.

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-356310 in HTML and CSAF.
CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, 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 these vulnerabilities has been reported to CISA

at this time.

5. UPDATE HISTORY

December 11, 2025: Initial Republication of Siemens ProductCERT SSA-356310

https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-09