America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Milesight UG65-868M-EA

Release Date: May 06, 2025 **Alert Code:** ICSA-25-126-02

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf>

1. EXECUTIVE SUMMARY

- **CVSS v4 6.1**
- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: Milesight
- **Equipment**: UG65-868M-EA
- **Vulnerability**: Improper Access Control for Volatile Memory Containing Boot Code

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow any user with admin privileges to inject arbitrary shell commands.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of UG65-868M-EA, an industrial gateway, are affected:

- UG65-868M-EA: Firmware versions prior to 60.0.0.46

3.2 VULNERABILITY OVERVIEW

3.2.1 Improper Access Control for Volatile Memory Containing Boot Code CWE-1274 <https://cwe.mitre.org/data/definitions/1274.html>

An admin user can gain unauthorized write access to the /etc/rc.local file on the device, which is executed on a system boot.

CVE-2025-4043 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.8 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:h/ui:n/s:c/c:n/i:h/a:n>).

A CVSS v4 score has also been calculated for CVE-2025-4043. A base score of 6.1 has been calculated; the CVSS vector string is (CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/SC:N/SI:H/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:h/ui:n/vc:n/vi:n/va:n/sc:n/si:h/sa:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Energy

- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** China

3.4 RESEARCHER

Joe Lovett of Pen Test Partners reported this vulnerability to CISA.

4. MITIGATIONS

Milesight released the latest firmware Version 60.0.0.46 for the UG65 gateway. Users can download the latest firmware from the Milesight download center. <https://www.milesight.com/iot/resources/download-center/#firmware-ug65>

Please contact Milesight technical support <https://www.milesight.com/company/contactus> for more information about this issue and for instructions for installing the latest firmware.

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

- Ensure that principles of least privilege are followed.
- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet <https://www.cisa.gov/uscert/ics/alerts/ics-alert-10-301-01>.
- 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), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is 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 <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices> on the ICS webpage on cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems>. 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 <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets <https://www.cisa.gov/sites/default/files/publications/cybersecurity_best_practices_for_industrial_control_systems.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

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

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

5. UPDATE HISTORY

- May 6, 2025: Initial Publication

Tags

Sector: Energy Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

MAY 08, 2025 **ICS ADVISORY | ICSA-25-128-02**

Hitachi Energy RTU500 Series </news-events/ics-advisories/icsa-25-128-02>

MAY 08, 2025 **ICS ADVISORY | ICSA-25-128-03**

Mitsubishi Electric CC-Link IE TSN </news-events/ics-advisories/icsa-25-128-03>

MAY 08, 2025 ICS ADVISORY | ICSA-25-128-01

Horner Automation Cscape </news-events/ics-advisories/icsa-25-128-01>

MAY 06, 2025 ICS ADVISORY | ICSA-25-126-01

Optigo Networks ONS NC600 </news-events/ics-advisories/icsa-25-126-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov