

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in ABB ALS-mini Load Controllers

Tracking #:432317844

Date:22-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical missing authentication vulnerability in ABB ALS-mini-S4/S8 IP intelligent load controllers, used in industrial energy management systems. The flaw allows unauthenticated remote access to the device's web interface, enabling attackers to view and modify configurations that could disrupt power distribution or load operations.

TECHNICAL DETAILS:

ABB has disclosed a critical vulnerability affecting its ALS-mini-S4 IP and ALS-mini-S8 IP intelligent load controllers used in industrial energy management and load balancing systems. The flaw, tracked as CVE-2025-9574, arises from a missing authentication mechanism in the device's embedded web server. Successful exploitation could allow unauthenticated remote attackers to access, view, or modify device configurations, potentially disrupting load control and power distribution processes.

Vulnerability Details

- **CVE-2025-9574**
- CVSS v4.0 Score: 9.9 (**Critical**)
- The embedded web server on ABB ALS-mini-S4 and ALS-mini-S8 IP controllers lacks authentication controls, allowing remote unauthenticated connections through the web interface. Attackers can modify operational parameters or configurations, which could result in partial or complete control of load management processes.
- Exploitation of this vulnerability could lead to:
 - Remote unauthorized modification of operational parameters.
 - Loss of configuration integrity and availability.
 - Potential manipulation of industrial load balancing and energy efficiency operations.

Affected Products

Product	Firmware Version	Serial Number Range	Support Status
ALS-mini-S4 IP	All versions	2000-5166	End-of-Life
ALS-mini-S8 IP	All versions	2000-5166	End-of-Life

ABB has confirmed that these products have reached end-of-support (EoL) status, and no security patches will be released.

RECOMMENDATIONS:

- Isolate affected devices from public networks.
- Restrict access to trusted IPs only.
- Enforce firewall and network segmentation.
- Monitor for unauthorized access attempts.
- Disable the web interface if not required.
- Consider replacing legacy EoL hardware with supported alternatives that include modern access control mechanisms.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://nvd.nist.gov/vuln/detail/CVE-2025-9574>