ADVANTECH Enabling an Intelligent Planet

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

SECURITY ADVISORY

Vulnerabilities Identified in WISE-4000LAN Series

This document summarizes the vulnerabilities identified in the WISE-4000LAN product line (WISE-4010LAN, WISE-4050LAN, WISE-4060LAN), the associated CVEs, and the remediation actions completed by Advantech.

Vulnerability Type, Impact and Solution

Item	CVE ID	Impact	Solution
1	CVE-2025-48461	Successful exploitation of the vulnerability could allow an unauthenticated attacker to conduct brute force guessing and account takeover as the session cookies are predictable, potentially allowing the attackers to gain root, admin or user access and reset passwords.	Users are advised to enable the existing **Security Mode**, which restricts high-risk services.
2	CVE-2025-48462	Successful exploitation of the vulnerability could allow an attacker to consume all available session slots and block other users from logging in, thereby preventing legitimate users from gaining access to the product.	Enabling **Security Mode** helps prevent session exhaustion and brute-force login attempts by minimizing the device's exposure to unauthorized access.
3	CVE-2025-48463	Successful exploitation of the vulnerability could allow an attacker to intercept data and conduct session hijacking on the exposed data as the vulnerable product uses unencrypted HTTP communication, potentially leading to unauthorised access or data tampering.	The built-in **Security Mode** disables HTTP access and improves communication security. Users should deploy devices behind a firewall or VPN and enable Security Mode after setup.
4	CVE-2025-48466	Successful exploitation of the vulnerability could allow an unauthenticated, remote attacker to send Modbus TCP packets to manipulate Digital Outputs, potentially allowing remote control of relay channel which may lead to operational or safety risks.	Firmware **A2.02 B00** introduces a new feature that allows users to disable **Modbus TCP** manually. By default, the function remains enabled. Users should also apply IP whitelisting via the built-in **ACL** feature to limit access.
5	CVE-2025-48467	Successful exploitation of the vulnerability could allow an attacker to cause repeated reboots, potentially leading to remote denial-of-service and system unavailability.	Firmware **A2.02 B00** includes enhanced validation to reject malformed Modbus packets and prevent device crashes. It is recommended to update to the latest firmware and limit Modbus access to trusted networks.
6	CVE-2025-48468	Successful exploitation of the vulnerability could allow an attacker that has physical access to interface with JTAG to inject or modify firmware.	In firmware **A2.02 B00**, the **JTAG interface is automatically disabled** during normal operation. It is also recommended to apply hardware-level protection such as epoxy sealing or fuse-locking

已註解 [SN1]: Annex D

已註解 [SN2]: Annex G

已註解 [SN3]: Annex H

已註解 [SN4]: Annex B

已註解 [SN5]: Annex E

已註解 [SN6]: Annex F

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

			before deployment.
7	CVE-2025-48469	Successful exploitation of the vulnerability could allow an unauthenticated attacker to upload firmware through a public update page, potentially leading to backdoor installation or privilege escalation.	Security Mode disables the firmware upload interface after initial setup. A popup message has been added to remind users to activate Security Mode as a best practice.
8	CVE-2025-48470	Successful exploitation of the stored cross-site scripting vulnerability could allow an attacker to inject malicious scripts into device fields and executed in other users' browser, potentially leading to session hijacking, defacement, credential theft, or privilege escalation.	Enabling **Security Mode** disables non-essential web services and reduces the risk of XSS exploitation. Additional improvements to input validation are planned for future firmware updates.

已註解 [SN7]: Annex A

已註解 [SN8]: Annex C

Credits

Advantech would like to thank the following researchers for responsibly disclosing the vulnerabilities:

- CVE-2025-48469: Lam Jun Rong
- CVE-2025-48466, CVE-2025-48470: Jay Turla, Japz Divino, Jerold Camacho
- CVE-2025-48461: Joel Chang Zhi Kai
- CVE-2025-48467, CVE-2025-48468, CVE-2025-48462: Marc Heuse
- CVE-2025-48463: Chua Wei Xun

Additionally, Advantech would like to thank CSA for their collaboration on the coordinated disclosure process.

Affected Products

We strongly recommend all users update their devices to this latest firmware version as soon as possible. The update is available for download on our official website

Model Name	Download Page
WISE-4060LAN	https://www.advantech.com/en/support/details/firmware-?id=1-1B835P3
WISE-4010LAN	
WISE-4050LAN	

Revision History

Version	Description	Release Date
1.0	First Advisory published	Jun. 24, 2025