Alcatel-Lucent Security Advisory No. SA-N0150 Ed. 02
OmniAccess Stellar WLAN APs – Multiple Vulnerabilities

Summary

ALE has released an AWOS maintenance release for the OmniAccess Stellar WLAN Access Points to address multiple security vulnerabilities. The vulnerabilities affect all OmniAccess Stellar Access Points running AWOS 5.0.2GA and earlier.

These vulnerabilities were discovered and reported by the Cyber Security Agency of Singapore.

References

Reference	CVE-2025-52687, CVE-2025-52687, CVE-2025-52689, CVE-2025-52690
Date	07/10/2025
Risk	Critical
Impact	take control, execute_arbitrary_code, confidentiality
Attack expertise	skilled, remote_no_account_no_user_interaction
Attack requirements	
CVSS score	9.8
Affected Products	OmniAccess Stellar Access Point Families - AP1100, AP1200, AP1300, AP1400. AP1500
Affected versions	AWOS 5.0.2GA and earlier
Fixed version	AWOS 5.0.2MR

Description of the Vulnerabilities

Java Script injection vulnerability in the OmniAccess Stellar web management interface (CVE-2025-52687)

Description: Incorrect checking of the text field in payloads that are input through the WebUI of the OmniAccess Stellar Access Point allows an attacker with administrator credentials for the access point to improperly injection Java script in the payload of web traffic. When other users visit the affected web page, the script is served to their browsers and executed in the context of their session which could lead to session hijacking, denial-of-service (DoS), and other attacks. To exploit this vulnerability, an attacker would need Administrator credentials.

Severity: Low

Attack Type: Network

CVSS 3.1 Base Score: 2.4

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N

Discovery: The vulnerability was discovered by the Cyber Security Agency of Singapore researchers Jay Turla, Japz Divino, and Jerold Camacho

Workaround: Manage OmniAccess Stellar APs using Enterprise Mode with OmniVista management platform and disable to web interface on the OmniAccess Stellar AP.

Resolution: Upgrade to AWOS 5.0.2MR1

Command injection vulnerabilities in the OmniAccess Stellar web management interface (CVE-2025-52687)

Description: The web management interface of the OmniAccess Stellar AP contains multiple vulnerabilities that allow improper command injections. Weakness in the processing of JSON methods submitted using the web

interface allows an attacker to inject commands that are executed with root privilege on the access point. The vulnerabilities could result in loss of the confidentiality, integrity, availability, and full control of the access point.

Severity: Critical

Attack Type: Network

CVSS 3.1 Base Score: 9.8

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Discovery: The vulnerability was discovered by the Cyber Security Agency of Singapore researchers Joel Chang Zhi Kai, Liu Yisen, Cao Wei, Lam Jun Rong, River Koh, Yeo Jun Yi Keith, and Hyunseok Yun

Workaround: Manage OmniAccess Stellar AP using Enterprise Mode with OmniVista management platform and disable to web interface on the OmniAccess Stellar AP.

Resolution: Upgrade to AWOS 5.0.2MR1

Weak session ID check in the OmniAccess Stellar web management interface (CVE-2025-52689)

Description: The web management interface of the OmniAccess Stellar AP uses a hard coded key to generate the API signature. This vulnerability could allow an attacker to craft a payload such that "/api/login" accepts the spoofed login request and returns a valid session ID with administrator privilege even though the attacker does not know the network administrator credentials. With this session ID the attacker can submit commands via the API interface to modify the behavior of the AP.

Severity: Critical

Attack Type: Network

CVSS 3.1 Base Score: 9.8

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Discovery: The vulnerability was discovered by the Cyber Security Agency of Singapore researchers Lam Jun Rong and Cao Yitian

Workaround: Manage OmniAccess Stellar AP using Enterprise Mode with OmniVista management platform and disable to web interface on the OmniAccess Stellar AP.

Resolution: Upgrade to AWOS 5.0.2MR1

Command injection vulnerabilities in the OmniAccess Stellar over UDP service (CVE-2025-52690)

Description: Improper checking of the packets received on the AP cluster interface causes the AP to be vulnerable to command injection attacks. This vulnerability allows an attacker to execute arbitrary commands as root resulting in a loss of the confidentiality, integrity, availability, and full control of the access point. To exploit this vulnerability, the AP must be in Express Mode.

Base Severity: High

Attack Type: Network

CVSS 3.1 Base Score: 8.1

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Discovery: The vulnerability was discovered by the Cyber Security Agency of Singapore researcher Lam Jun Rong

Workaround: Manage OmniAccess Stellar AP using Enterprise Mode with OmniVista management platform.
Resolution: Upgrade to AWOS 5.0.2MR1

Status on Alcatel-Lucent Enterprise Products

The ALE products that are impacted by the vulnerabilities are identified below.

Product Name	Release
OmniAccess Stellar Access Point Families - AP1100, AP1200, AP1300, AP1400. AP1500	AWOS 5.0.2GA or earlier

Workarounds

The relevant workaround is defined in the detailed description of each vulnerability above.

Resolution for Alcatel-Lucent Enterprise affected products

Information on software versions to address the vulnerabilities is provided below.

Product	Fixed in	Date
OmniAccess Stellar Access Point Families - AP1100, AP1200, AP1300, AP1400. AP1500	AWOS 5.0.2MR	June 2025

History

Ed.01 (2025 July 10): creation
Ed.01 (2025 July 11): update to credit researchers who discovered the vulnerabilities