مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Planet Technology Network Devices

Tracking #:432317123

Date:25-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple critical vulnerabilities have been identified in Planet Technology network devices used in industrial environments.

TECHNICAL DETAILS:

Recent research has uncovered multiple critical vulnerabilities in Planet Technology network devices, including industrial network switches and the UNI-NMS-Lite network management system. These flaws allow attackers to execute arbitrary commands, bypass authentication, and obtain full administrative access—often remotely and with low attack complexity.

Several vulnerabilities stem from hard-coded credentials and improper input handling, exposing organizations, especially those in critical manufacturing and operational technology (OT) environments, to significant risk. Immediate action is required to mitigate these threats, as exploitation could lead to unauthorized device control, data manipulation, and disruption of critical infrastructure.

Key Vulnerabilities:

CVE	Weakness (CWE)	CVSS v3 Score	Description
CVE-2025-46271	CWE-78 (OS Command Injection)	9.1 (Critical)	Pre-authentication command injection in UNI-NMS-Lite, enabling remote code execution.
CVE-2025-46272	CWE-78 (OS Command Injection)	9.1 (Critical)	Post-authentication command injection in WGS switches, allowing OS command execution.
CVE-2025-46273	CWE-798 (Hard-coded Credentials)	9.8 (Critical)	Hard-coded MQTT credentials ("client:client") in NMS and devices, granting admin access.
CVE-2025-46274	CWE-798 (Hard-coded Credentials)	9.8 (Critical)	Hard-coded MongoDB credentials ("planet:123456") in NMS, exposing database access.
CVE-2025-46275	CWE-306 (Missing Authentication)	9.8 (Critical)	Authentication bypass in WGS switches, enabling unauthorized admin account creation.

AFFECTED PRODUCTS:

The following versions of Planet Technology products are affected:

- UNI-NMS-Lite: Versions 1.0b211018 and prior
- NMS-500: All Versions
- NMS-1000V: All Versions
- WGS-804HPT-V2: Versions 2.305b250121 and prior
- WGS-4215-8T2S: Versions 1.305b241115 and prior

Planet Technology has released patches for the following devices:

- WGS-804HPT (v2)
- WGS-4215-8T2S

- UNI-NMS
- NMS-500
- NMS-1000V

RECOMMENDATIONS:

- **Patch and Update:** Apply firmware and software updates provided by Planet Technology as soon as available.
- **Change Default Credentials:** Replace all default and hard-coded credentials on affected devices and management systems.
- **Restrict Network Access:** Limit access to management interfaces and NMS systems to trusted networks only. Use firewalls and network segmentation.
- **Monitor for Exploitation:** Implement intrusion detection and monitor logs for unusual activity, especially unauthorized admin account creation or configuration changes.
- **Disable Unused Services:** Turn off remote management and unnecessary services where possible.
- **Incident Response Readiness:** Prepare to respond to potential exploitation, including isolating affected devices and restoring from clean backups

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://www.cisa.gov/news-events/ics-advisories/icsa-25-114-06