مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Planet WGS-804HPT Switches

Tracking #:432316763

Date:20-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed three critical vulnerabilities have been discovered in Planet Technology's WGS-804HPT industrial switches, which are widely used in building and home automation systems.

TECHNICAL DETAILS:

Three critical vulnerabilities have been discovered in Planet Technology's WGS-804HPT industrial switches, which are widely used in building and home automation systems.

These flaws, when chained together, allow unauthenticated remote code execution, posing a significant threat to industrial networks and connected IoT devices. The vulnerabilities affect the dispatcher.cgi interface of the switches' web service and include:

- CVE-2024-48871 (CVSS 9.8): Stack-based buffer overflow
- CVE-2024-52320 (CVSS 9.8): OS command injection
- CVE-2024-52558 (CVSS 5.3): Integer underflow

Successful exploitation could allow attackers to hijack execution flow, execute arbitrary OS commands, and potentially gain control over the device and connected networks

Fixed Versions:

- Firmware Version Planet Technology has released firmware version 1.305b241111 to patch these vulnerabilities.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends users of Planet WGS-804HPT switches are strongly urged to upgrade to the fixed firmware version.

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.planet.com.tw/en/support/downloads?method=keyword&keyword=v1.305b241111