مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerabilities in Planet Industrial Switch

Tracking #:432316607

Date:09-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Planet Technology has disclosed three vulnerabilities in their industrial switch product, Planet WGS-804HPT.

TECHNICAL DETAILS:

Planet Technology has disclosed three vulnerabilities in their industrial switch product, Planet WGS-804HPT. These vulnerabilities, CVE-2024-48871, CVE-2024-52320, and CVE-2024-52558, expose the product to serious remote code execution (RCE) risks

Vulnerability Overview:

- **CVE-2024-48871 - Stack-based Buffer Overflow (CWE-121):**
  - The product is vulnerable to a stack-based buffer overflow, where an attacker could send a malicious HTTP request. The webserver fails to properly validate the input size before copying data into the stack, potentially allowing remote code execution.
  - **CVSS v4 Base Score:** 9.3
- **CVE-2024-52320 - OS Command Injection (CWE-78):**
  - This vulnerability allows an attacker to send arbitrary OS commands through a malicious HTTP request. This could result in remote code execution, leading to unauthorized actions on the device.
  - **CVSS v4 Base Score:** 9.3
- **CVE-2024-52558 - Integer Underflow (CWE-191):**
  - This vulnerability occurs when an unauthenticated attacker sends a malformed HTTP request, causing an integer underflow condition. This can lead to a crash in the program, disrupting its normal functionality.
  - **CVSS v4 Base Score:** 6.9

- **Affected Product and Version:** Planet WGS-804HPT v1.305b210531
- **Fixed Versions:**1.305b241111 or later

RECOMMENDATIONS:

- Users are urged to upgrade to fixed version to address the vulnerabilities.

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