مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Multiple vulnerabilities in PLANET Technology Switch Devices

Tracking #:432316347

Date:01-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities have been identified in PLANET Technology switches that could allow unauthorized access, data theft, and denial of service.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in PLANET Technology switches, spanning hard-coded credentials, cleartext password storage, CSRF, XSS, missing authentication, weakly encoded passwords, insecure hash functions, and Denial of Service (DoS).

Identified Vulnerabilities:

- **Cross-Site Request Forgery (CSRF) (CVE-2024-8458):** Enables attackers to execute unauthorized actions on behalf of authenticated users.
- **Cross-Site Scripting (XSS) (CVE-2024-8457):** Injection of malicious scripts into web pages viewed by other users, potentially leading to data theft or session hijacking.
- **Missing Authentication (CVE-2024-8456, CVSS 9.8):** Absence of proper access controls, allowing unauthorized access to critical functionalities such as firmware upload and download.
- **Weakly Encoded Passwords (CVE-2024-8455):** Insecure password encoding, making them susceptible to cracking attempts.
- **Insecure Hash Functions (CVE-2024-8452, CVE-2024-8453):** Use of outdated hashing algorithms, compromising the security of stored credentials.
- **Denial of Service (DoS) (CVE-2024-8454, CVE-2024-8451):** Vulnerabilities that could be exploited to disrupt or render the devices unavailable.

Affected Products:

- GS-4210-24PL4C (hardware 2.0)
- GS-4210-24P2S (hardware 3.0)
- IGS-5225-4UP1T2S (hardware 1.0) – End of Life

Mitigation Steps:

- GS-4210-24PL4C (hardware 2.0): Version 2.305b240719 or later
- GS-4210-24P2S (hardware 3.0): Version 3.305b240802 or later
- The IGS-5225-4UP1T2S has reached its End of Life and is no longer supported. Replacement is recommended

RECOMMENDATIONS:

- Apply Updates Promptly: Update all affected devices to the latest firmware versions without delay.
- Monitor Network Activity: Increase monitoring and employ intrusion detection systems to identify suspicious activity.
- Review Security Policies: Enforce strong password policies and access controls.
- Consider Replacement: Evaluate replacing end-of-life devices to ensure ongoing security and support.

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://nvd.nist.gov/vuln/detail/CVE-2024-8456