مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in D-Link NAS Devices

Tracking #:432316495

Date:11-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in D-Link NAS devices that could potentially be exploited to execute malicious code on affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-10914**
- CVSSv4 score of 9.2 Critical
- A critical command injection vulnerability exists in multiple D-Link NAS device models. This flaw allows remote attackers to execute arbitrary commands on affected devices without authentication, potentially leading to unauthorized access, data theft, and system compromise.
- The vulnerability resides in the account_mgr.cgi script, specifically in the name parameter of the cgi_user_add command. Malicious actors can exploit this flaw by crafting HTTP GET requests containing specially formatted input. This input is not properly sanitized, allowing attackers to inject arbitrary shell commands and execute them on the target device.
- Successful exploitation of CVE-2024-10914 can result in:
    - Unauthorized access to the NAS device
    - Execution of arbitrary commands with root privileges
    - Data theft or manipulation
    - Potential deployment of malware

Affected Products and Versions:

- DNS-320 Version 1.00
- DNS-320LW Version 1.01.0914.2012
- DNS-325 Version 1.01, Version 1.02
- DNS-340L Version 1.08

RECOMMENDATIONS:

- **Apply firmware updates**: Install the latest firmware updates provided by D-Link as soon as they become available
- **Restrict Network Access**: Limit access to the NAS management interface to trusted IP addresses only.
- **Monitor for Updates**: Stay vigilant for upcoming security patches from D-Link
- **Network Segmentation**: If possible, isolate affected NAS devices from the internet and critical network segments.
- **Regular Security Audits**: Conduct frequent security assessments of network infrastructure, including NAS devices.

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-2024-10914