Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Flaw in D-Link NAS Devices Exposes Thousands to Remote Command Attacks

Date of Publication	Admiralty Code	TA Number
November 14, 2024	A1	TA2024430

Summary

First Seen: November 2024
Affected Products: D-Link NAS devices
Impact: A critical security vulnerability, CVE-2024-10914, is putting thousands of D-Link NAS devices at serious risk worldwide. This flaw, found in the `account_mgr.cgi` script, allows attackers to remotely execute arbitrary commands by sending tailored HTTP GET requests. With over 61,000 systems potentially exposed, this vulnerability presents a substantial risk of unauthorized access and control over affected devices.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-10914	D-Link NAS Command Injection Vulnerability	D-Link NAS devices	✗	✗	✗

Vulnerability Details

#1 A critical vulnerability, CVE-2024-10914, is currently being exploited by attackers, impacting numerous end-of-life D-Link NAS models. This command injection flaw has exploit code readily available, leaving these devices particularly vulnerable to unauthorized access and command execution.

#2 The vulnerability, located in the `account_mgr.cgi` URI, originates from improper input handling of the `name` parameter within the `cgi_user_add` command of the CGI script. Due to insufficient sanitization, unauthenticated attackers can exploit this flaw to inject and execute arbitrary shell commands. By sending carefully crafted HTTP GET requests to the NAS device, attackers can manipulate the `name` parameter to remotely execute malicious commands.

#3

It is estimated that over 61,000 vulnerable D-Link NAS devices are currently active on the internet, primarily in small business environments. Given that these devices are classified as end-of-life (EOL), they will not receive any security updates or patches from D-Link. This highlights the importance of effective device management, especially for outdated hardware.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-10914	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	cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-320lw_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-325_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:dns-340l_firmware:*:*:*:*:*:*:*:*	CWE-77

Recommendations

Retire and Replace: If you own any of the affected D-Link NAS devices (DNS-320, DNS-320LW, DNS-325 and DNS-340L), it's crucial to retire these devices immediately. Since D-Link no longer supports them and there are no available patches to fix the vulnerabilities, continued use poses a significant security risk.

Upgrade to Supported devices: Replace the retired devices with newer, supported NAS devices from reputable manufacturers. Ensure that the new devices receive regular security updates and firmware patches to mitigate future vulnerabilities.

Data Backup: Before retiring the affected NAS device, ensure that all important data stored on it is backed up securely. This will prevent data loss and facilitate the transition to a new NAS device. Backup solutions could include cloud storage, external hard drives, or network backups to another secure location.

Limit NAS Access to Trusted IPs: As a temporary solution, it's recommended to limit access to the NAS management interface to trusted IP addresses only. This will help reduce the risk of unauthorized access while users take steps to secure or replace the affected devices.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1588.005 Exploits	T1059 Command and Scripting Interpreter		

Patch Details

As no patches are available for CVE-2024-10914, which affects D-Link NAS devices (DNS-320, DNS-325, and DNS-340L), and these devices are no longer supported, users should prioritize replacing them with newer, supported NAS models to maintain security.

References

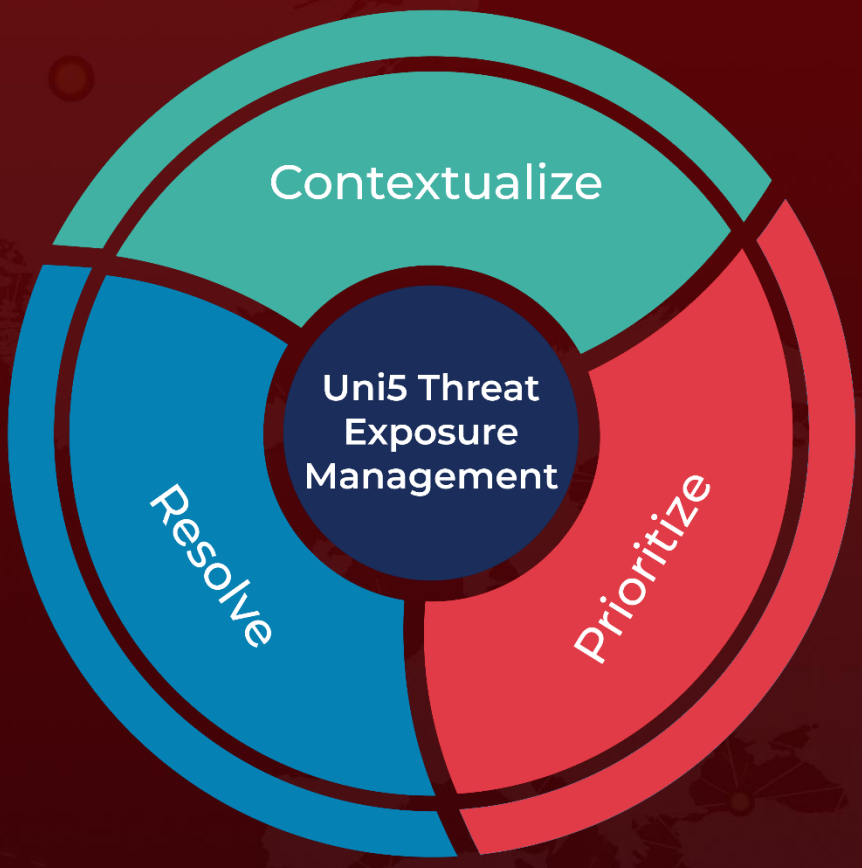
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10413

https://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 14, 2024 . 4:30 AM

More at www.hivepro.com