Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical RCE Flaw Found in EoL D-Link NAS Devices

Date of Publication	Admiralty Code	TA Number
April 9, 2024	A1	TA2024134

Summary

First Seen: March 26, 2024
Affected Platform: Over 92,000 D-Link NAS devices, including DNS-340L, DNS-320L, DNS-327L, and DNS-325, are exposed online and vulnerable.
Impact: A critical vulnerability (CVE-2024-3273) in certain D-Link NAS devices poses a serious threat, as they're no longer supported, leaving them vulnerable to attacks. Successful exploitation could lead to unauthorized access, data theft, system modifications, or denial of service attacks, emphasizing the urgency to retire affected devices for data protection.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-3273	D-Link NAS Remote Code Execution Vulnerability	Multiple D-Link NAS devices	✗	✗	✓

Vulnerability Details

#1 A critical security vulnerability, identified as CVE-2024-3273, has been discovered in certain D-Link NAS devices. These devices, including DNS-320L, DNS-325, DNS-327L, and DNS-340L, are particularly concerning because they are no longer supported by D-Link. This means they won't receive security updates to address this or other vulnerabilities that may be found.

#2 The vulnerability resides in a program on the NAS device called nas_sharing.cgi. Attackers can exploit this vulnerability in two ways. First, they can leverage a built-in backdoor with a hardcoded username and password to gain unauthorized access to the device. Second, they can exploit a command injection vulnerability to run malicious commands directly on the NAS, potentially allowing them to steal sensitive data stored on the device.

#3 Threat actors are exploiting this vulnerability for the distribution of Mirai malware variants, such as skid.x86, which form botnets for large-scale DDoS attacks. Since these D-Link NAS devices are no longer supported and there are no patches available, the only way to mitigate the risk of this vulnerability is to retire the affected device. It's highly recommended to replace it with a newer, supported NAS model to ensure your data is protected.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-3273	DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013 DNS-325 Version 1.01 DNS-327L Version 1.09, Version 1.00.0409.2013 DNS-340L Version 1.08	cpe:2.3:a:d-link:dns-320l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-325:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-327l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-340l:*:*:*:*:*:*:*:*	CWE-77

Recommendations

Retire and Replace: If you own any of the affected D-Link NAS devices (DNS-320L, DNS-325, DNS-327L, 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.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0001 Initial Access	T1059 Command and Scripting Interpreter
T1588 Obtain Capabilities	T1543 Create or Modify System Process	T1588.005 Exploits	T1588.006 Vulnerabilities
T1203 Exploitation for Client Execution	T1498 Network Denial of Service		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	859e679f8e8be4a4c895139fb7fb1b177627bbe712e1ed4c316ec85008426db8
IPv4	38[.]6[.]224[.]248

Patch Details

No patches are available for the CVE-2024-3273 vulnerability affecting D-Link NAS devices DNS-320L, DNS-325, DNS-327L, and DNS-340L. As these devices are no longer supported, users are advised to retire them and replace with newer, supported NAS devices for security.

Link:
https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

References

https://www.greynoise.io/blog/cve-2024-3273-d-link-nas-rce-exploited-in-the-wild

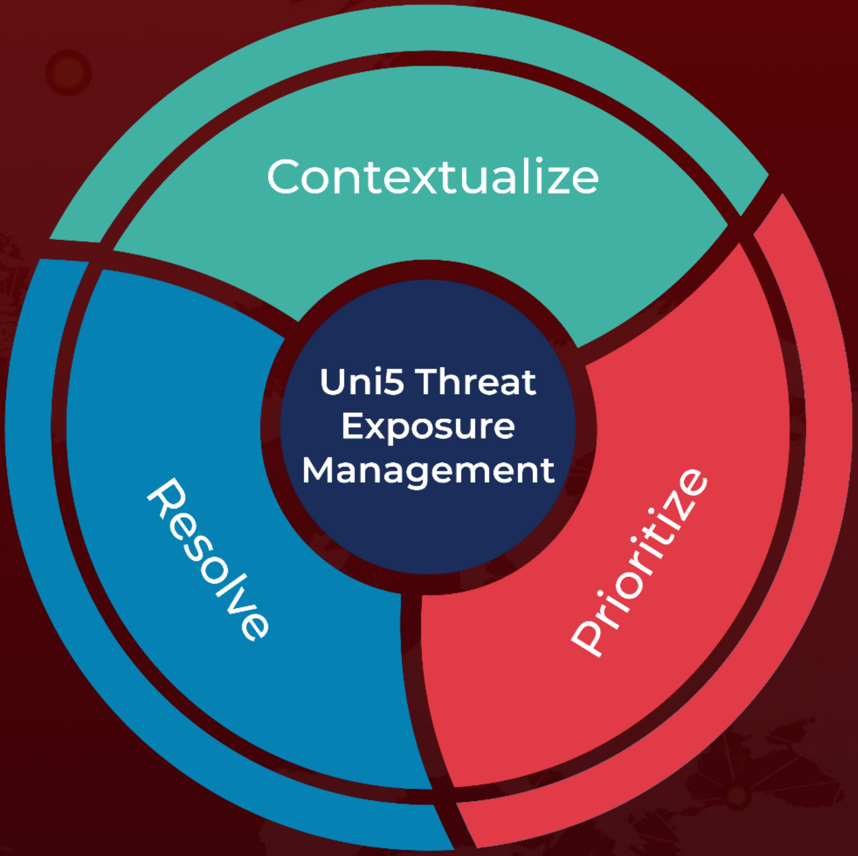
https://github.com/netsecfish/dlink

https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-92-000-d-link-nas-devices-now-exploited-in-attacks/

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

April 9, 2024 • 6:30 AM

More at www.hivepro.com