Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

08 April 2024

D-Link DNS Vulnerabilities

CVE-2024-3272 | CVE-2024-3273 | RCE | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of severe critical vulnerabilities under active exploitation known as CVE-2024-3272 and CVE-2024-3273.[1] The vulnerabilities affect D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403.[2] Exploitation of the vulnerabilities may allow an attacker to remotely commandeer the vulnerable devices by sending a set of HTTP requests to them.[3] Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the system, potentially leading to unauthorized access to sensitive information, modification of system configurations, or denial of service conditions.[4]

The Cal-CSIC recommends immediately using an alternate device as the vulnerable D-Link devices have reached end of life/end of service and will not be patched.

For further information on D-LINK DNS exploit proof of concept please refer to, Net Sec Fish D-Link exploit.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

	help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Ars Technica; "Critical takeover vulnerabilities in 92,000 D-Link devices under active exploitation;" https://arstechnica.com/security/2024/04/hackers-actively-exploit-critical-remote-takeover-vulnerabilities-in-d-link-devices/; accessed 08 April 2024

[2] D-Link; "DNS-320L / DNS-325 / DNS-327 / DNS-340L and All D-Link NAS Storage :: All Models and All Revison :: End of Service Life :: CVE-2024-3273 : Vulnerabilities Reported by VulDB/Netsecfish;" https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383; accessed 08 April 2024

[3] Grey Noise; "D-LINK NAS CVE-2024-3273 RCE ATTEMPT;" https://viz.greynoise.io/tags/d-link-nas-cve-2024-3273-rce-attempt?days=30; accessed 08 April 2024

[4] HelpNet Security; "92,000+ internet-facing D-Link NAS devices accessible via "backdoor" account (CVE-2024-3273)" https://www.helpnetsecurity.com/2024/04/08/cve-2024-3273/; accessed 08 April 2024

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.