

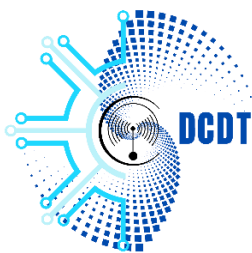
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

9 September 2026

Advisory 283: D-Link DNS-3xxL NAS Series Multiple OS Command Injection Vulnerabilities (CVE-2026-82689, CVE-2026-82692, and CVE-2026-85223).

Release Date: 31st August 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and members of the general public that use a D-Link DNS-320L, DNS-327L, DNS-340L, or DNS-345 network-attached storage (NAS) device. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-82689, CVE-2026-82692, and CVE-2026-85223 are three OS command injection vulnerabilities in the web-management CGI scripts of D-Link's DNS-3xxL ShareCenter NAS series, a mass-market consumer/small-office storage line sold through general electronics retailers worldwide. CVE-2026-82689 affects /cgi-bin/isomount_mgr.cgi (the "upIsoRootPath" parameter) on DNS-320L, DNS-327L, DNS-340L, and DNS-345; CVE-2026-82692 affects /cgi-bin/iscsi_mgr.cgi (the "alias"/"username"/"password"/"volume_location" parameters) on DNS-340L and DNS-345; and CVE-2026-85223 affects /cgi-bin/dropbox.cgi (the "callback_url"/"sync_interval" parameters) on DNS-340L specifically. All three allow a remote, low-privileged attacker to inject and execute arbitrary operating system commands.

What are the systems affected?

The following version(s) are affected:

- D-Link DNS-320L, DNS-327L, DNS-340L, and DNS-345, firmware up to 20260717 – (Affected - CVE-2026-82689)
- D-Link DNS-340L and DNS-345, firmware up to 20260717 - (Affected - CVE-2026-82692); D-Link DNS-340L firmware 1.01B04 - (Affected - CVE-2026-85223)

No fixed firmware exists or will be issued - all listed models are formally End-of-Life/End-of-Service. D-Link has confirmed these models will not receive a security patch under any circumstances, since they are formally End-of-Life/End-of-Service. Organizations and individuals running any of these devices should treat replacement, not patching, as the actual remediation.

What does this mean?

Typical attack flow:

1. **Reach the device's web-management CGI scripts**
 - An attacker with low-level access to the NAS device's web-management interface - for example, a weak or default account, or reachability from an untrusted network segment - sends a crafted request to one of the affected CGI scripts (isomount_mgr.cgi, iscsi_mgr.cgi, or dropbox.cgi) with a malicious parameter value.
2. **Execute arbitrary OS commands**
 - Because the affected scripts pass the parameter value into a system command without sanitisation, the attacker's injected command executes with the privileges of the web-management process, using publicly available proof-of-concept exploit code.

Attack vectors:

- A network-based attack against any reachable, unpatched DNS-3xxL device's web-management interface, requiring only low-level access to that interface (CVSS PR:L).
- No user interaction is required, and public exploit code already exists for all three vulnerabilities.

Successful exploitation may allow attackers to:

- Execute arbitrary operating system commands on the NAS device, potentially reading, modifying, or destroying any data it stores.
- Use a compromised NAS device as a foothold into the wider home or organizational network it is connected to, or recruit it into a botnet.

Mitigation process

CERTVU recommends the following:

1. Retire and replace affected devices

- Since D-Link has confirmed no patch will be issued for these End-of-Life models, plan to decommission and replace any DNS-320L, DNS-327L, DNS-340L, or DNS-345 device with a currently-supported product.

2. Immediately disconnect from the internet if replacement is not yet possible
3. Restrict management-interface access as an interim measure
4. Back up and migrate data promptly

Report any suspected compromise of a D-Link DNS-3xxL device, or unusual network behaviour on a network using one, to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-82689>
2. <https://www.cve.org/CVERecord?id=CVE-2026-82692>
3. <https://www.cve.org/CVERecord?id=CVE-2026-85223>