NCA-07.050824: National CERT Advisory – D-Link Critical Vulnerability

Introduction

A critical vulnerability has been identified in multiple D-Link NAS (Network Attached Storage) devices, including models DNS-340L, DNS-320L, DNS-327L, and DNS-325, among others. This vulnerability stems from issues within the “nas_sharing.cgi uri”, specifically involving hardcoded credentials and a command injection vulnerability via the system parameter. Exploitation of this vulnerability could lead to arbitrary command execution on affected devices, potentially granting attackers access to sensitive information, alteration of system configurations, or denial of service.

Impact

The exploitation of this vulnerability poses a significant risk to affected D-Link NAS devices. Attackers could gain unauthorized access, manipulate system settings, or disrupt services, potentially resulting in data breaches or system downtime.

Vulnerable Systems

The following CVEs have been identified as affecting D-Link NAS devices:

- **CVE-2024-3273**: High severity, affecting DNS-320L, DNS-325, DNS-327L, and DNS-340L models up to April 3, 2024.
- **CVE-2024-3272**: Critical severity, impacting DNS-320L, DNS-325, DNS-327L, and DNS-340L models up to April 3, 2024.

Recommendations

NCERT strongly advises administrators to take the following actions:

1. Apply vendor-provided patches to all affected devices as soon as possible, following the instructions provided by D-Link.
2. Regularly monitor for updates and security advisories from D-Link and other relevant sources.
3. Implement robust network security measures to detect and prevent unauthorized access to vulnerable devices.
4. Restrict network access to affected devices to only essential users and services.
5. Consider implementing network segmentation to isolate vulnerable devices from critical infrastructure.

References

For further information and assistance, please refer to the following resources:

- **D-Link Security Announcement**: [https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383]
- **Github - dlink**: [https://github.com/netsecfish/dlink]
- **VulDB**: [https://vuldb.com/?ctiid.259284]
- **Tenable**: [https://www.tenable.com/cve/CVE-2024-3273]

NCERT emphasizes the criticality of addressing this vulnerability promptly to mitigate potential risks to organizational assets and data. Network Administrators are urged to prioritize these recommendations to ensure the security and integrity of their network infrastructure.