

Vulnerability Overview

D-Link DNS-320 ShareCenter

Unauthenticated remote code execution (CVE-2019-16057)

Vulnerability Rating

Critical

CVSS v2 10.0



REMOTE CODE EXECUTION

Introduction

D-Link DNS-320 ShareCenter is a network-attached storage (NAS) device with a web-based management interface. CyStack identified a critical remote command injection flaw in the device's login handling logic that can allow unauthenticated remote code execution

Synopsis

CVE-2019-16057 is a CWE-78 (OS command injection) issue in login_mgr.cgi on D-Link DNS-320 devices running affected firmware. Successful exploitation enables a remote attacker to execute arbitrary commands, leading to full device compromise (confidentiality, integrity, and availability impact).

Affected Devices

This vulnerability affected the DNS-320 line of products. The manufacturer suggested the number of units affected by this firmware flaw might be up to **61,000 devices connected to the internet**.

Details

The vulnerability stems from insufficient sanitization of user-controlled input in login_mgr.cgi. CyStack's analysis shows a hidden "SSL Login" feature where the port parameter can be "poisoned" to inject shell metacharacters and execute system commands. Exploitation is remote and unauthenticated, and can result in command execution with root-level control of device functions.

Timeline

- **August 14, 2019:** CyStack reports the issue to D-Link.
- **August 15, 2019:** The manufacturer first response and detailing
- **September 06, 2019:** D-Link team confirms the vulnerability and works on a patch
- **September 07, 2019:** CVE-2019-16057 assigned to the vulnerability
- **September 11, 2019:** D-Link team includes CVE in release notes and allow disclosure
- **September 15, 2019:** D-Link publishes vendor advisory SAP10123

Learn more

[CyStack Advisories](#)

[NIST Vulnerability Database](#)

[Vendor Announcement](#)