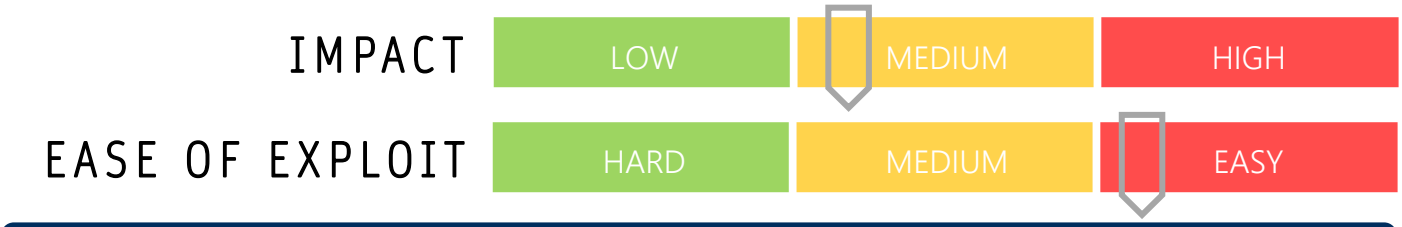
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00081

D-LINK ROUTER ZERO DAY FLAW

DATE ISSUED: 15th December 2020



OVERVIEW

A number of D-Link VPN routers may be susceptible to a zero-day flaw allowing attackers to gain administrator access and perform remote device takeover due to flawed firmware.

BREAKDOWN

Models DSR-150, DSR-250, DSR-500 and DSR-1000AC running the firmware versions 3.14 and 3.17 may be susceptible to a attack which relies on three chained bugs identified by Digital Defense researchers. The flawed links in the chain are unauthenticated remote LAN/WAN root command injection, authenticated root command injection and an authenticated crontab injection. While there is no full solution to resolve theses issues, D-Link have issued a series of firmware patches and hotfixes to mitigate the risk of compromise.

CVE-2020-25757, CVE-2020-25759, CVE-2020-25758

REMEDIATION STEPS

- Apply available beta firmware patches and hot patched provided by D-Link and check regularly for full security patches to be installed when they become available. Expected release Mid December 2020

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/d-link-routers-zero-day-flaws/162064/
D-Link: https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10195