Raport consolidat eveniment cibernetic

Vulnerabilitate RCE în Routerele VPN D-Link EoL

D-Link a emis un avertisment privind o vulnerabilitate de execuție de cod la distanță (**RCE**) care afectează routerele VPN din seria **DSR-150/150N** și **DSR-250/250N**. Această vulnerabilitate este neautentificată și nu va fi remediată, întrucât dispozitivele au atins statutul de **End of Life (EoL)** și **End of Support (EoS)** la data de **1 mai 2024.**

Informații suplimentare

TIP	Remote Code Execution (RCE) fără autentificare.
Dispozitivele afectate	• DSR-150 / DSR-150N • DSR-250 / DSR-250N
Versiunea	De la **3.13** până la **3.17B901C**.
Impact	Exploatarea permite unui atacator să controleze complet dispozitivul afectat. Acest lucru poate conduce la: • Compromiterea rețelelor conectate. • Distribuirea de malware prin rețea. • Risc pentru datele și echipamentele conectate.
Poziția D-Link	D-Link a confirmat că nu va lansa patch-uri pentru această vulnerabilitate, recomandând utilizatorilor: • Înlocuirea routerele afectate cu modele mai noi și cu suport activ. • Utilizarea ultimei versiuni de firmware disponibile (deși aceasta nu protejează împotriva defectului RCE).

Metodologie de exploatare	Atacatorul identifica routerele vulnerabile prin scanări automate și ulterior transmite cereri HTTP/HTTPS manipulate pentru a executa cod pe dispozitiv.
IOC	1. Trafic neautorizat provenit de la dispozitivul afectat. 2. Configurații modificate în mod neașteptat. 3. Creșteri anormale de trafic către endpoint-uri externe necunoscute.
Măsuri de remediere	**Recomandările oferite de către D-Link** 1. Retragerea și înlocuirea dispozitivelor afectate **DSR-150/150N și DSR-250/250N** cu modele de D-Link ce dețin suport activ. 2. Actualizarea firmware de pe pagina Legacy D-Link pentru: **DSR-150, DSR-150N, DSR-250, DSR-250N.** **Mitigări temporare** 1. Restricționarea accesului la interfața de administrare prin configurarea firewall-urilor pentru a permite acces doar din rețele de încredere. 2. Dezactivarea serviciilor neutilizate prin închiderea porturilor expuse către internet, dar care nu sunt esențiale. 3. Segmentarea rețelei prin plasarea routerele vulnerabile într-o zonă izolată pentru a limita impactul unui potențial atac. 4. Monitorizare activă a traficului pentru a detecta comportamente anormale.

Resurse externe

https://www.bleepingcomputer.com/news/security/d-link-urges-users-to-retire-vpn-routers-impacted-by-unfixed-rce-flaw/

https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10415