Raport consolidat eveniment cibernetic

CVE-2024-20480

CVE-2024-20480 este o vulnerabilitate în funcționalitatea *DHCP Snooping* din software-ul ***Cisco IOS XE,*** care afectează *edge nodes* ale rețelei *Software-Defined Access (SD-Access).*

Vulnerabilitatea permite unui atacator neautentificat, aflat la distanță, să trimită pachete *IPv4 DHCP* malformate către dispozitivul afectat, determinând utilizarea excesivă a resurselor CPU și, în final, o stare de DoS ce necesită o repornire manuală a dispozitivului pentru recuperare.

Informații suplimentare

TIP	**CVE-2024-20480**
CVE relevante identice	CVE-2024-20259 CVE-2024-20481
Vectorul de atac	Exploatarea se efectuează prin trimiterea unui volum mare de pachete IPv4 DHCP către dispozitivul afectat.
Condițiile de exploatare	• Dispozitivele afectate trebuie să folosească *DHCP Snooping*. • Atacatorul necesită acces la rețea în care se află dispozitivul afectat. • Atacul poate fi realizat de către orice entitate care are acces la rețea, fără a fi nevoie de un cont sau privilegii speciale pe dispozitivul țintă. • Expedierea unui flux de pachete *IPv4 DHCP* malformate sau cu conținut specific către dispozitivul afectat, ce determină consumul resurselor *CPU* și întreruperea traficului de rețea. • Lipsa unui Patch de securitate aplicat actualizat la zi.
Instrumente de analiză	• Scanarea vulnerabilității cu ajutorul la *Nessus* comanda: “**nessuscli update --plugins** **nessuscli scan list** **nessuscli scan run --target <IP-ul dispozitivului Cisco> --policy "Cisco Device Vulnerability Detection"”** sau cu ajutorul la OpenVAS. • Monitorizarea traficului cu ajutorul la Wireshark cu ajutorul comenzii: **“sudo wireshark -k -i eth0 -f "udp port 67 or udp port 68"”**

	• Monitorizarea performanța rețelei cu ajutorul la *SolarWinds Network* sau indentificarea anomalii cu ajutorul la *Cisco NetFlow Analyzer.* • Folosirea instrumente SIEM care colectează și corelează datele. • Testarea comportamentul dispozitivelor prin folositea *Metasploit Framework*: “**use auxiliary/dos/cisco/ios_dhcp_dos** **set RHOSTS <IP-ul dispozitivului Cisco>** **set PAYLOAD malform_dhcp** **run”** *Scapy comandă:* **“from scapy.all import *** **dhcp_packet = Ether()/IP(dst="255.255.255.255")/UDP(sport=68, dport=67)/BOOTP(op=1)/DHCP(options=[("message-type", "discover")])** **sendp(dhcp_packet, iface="eth0")”**
Recomandări generice	• Aplicarea patch-urilor furnizate de Cisco cît mai curând posibil. • Configurarea firewall-urile și filtrele de acces pentru a limita traficul DHCP. Utilizarea sistemelor de detectare și monitorizare.

Resurse externe

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-MBcbG9k