Raport consolidat eveniment cibernetic

Vulnerabilitate Cisco Root Command Execution

Vulnerabilitatea descoperită în dispozitivele Cisco permite unui atacator neautentificat să injecteze comenzi la nivel de sistem cu privilegii administrative complete, ceea ce poate duce la:

- Accesul complet la datele și funcțiile dispozitivului;
- Modificări în configurarea rețelei;
- Posibilitatea de a lansa atacuri suplimentare din rețea sau chiar compromiterea întregii infrastructuri.

Informații suplimentare

TIP	Command Injection
Produsele afectate	❖ **Cisco IOS și IOS XE** - Versiuni de software pentru echipamente de rețea, inclusiv rutere și switch-uri. ❖ **Cisco ASA (Adaptive Security Appliance)** - Soluție de firewall, utilizată în securizarea perimetrului de rețea. ❖ **Cisco NX-OS** - Software-ul pentru echipamente de tip data center și switch-uri de înaltă performanță.
Nivel de criticitate	Critic (posibil scor **CVSS 9-10**), deoarece permite escaladarea privilegiilor și accesul complet la sistem.
Impactul vulnerabilității	Această vulnerabilitate este extrem de critică datorită accesului root obținut de către atacatori. Principalele riscuri sunt: ❖ **Acces neautorizat**: Un atacator poate obține acces deplin la dispozitiv, permițându-i să citească și să modifice configurațiile și datele. ❖ **Persistență**: Obținerea accesului root poate permite atacatorului să instaleze backdoor-uri sau alte mijloace pentru a menține accesul pe termen lung. ❖ **Risc de escaladare**: Un atacator poate folosi dispozitivul compromis pentru a lansa atacuri suplimentare asupra altor sisteme conectate în rețea. ❖ **Expunerea datelor sensibile**: Datele stocate pe dispozitiv și traficul de rețea pot fi monitorizate sau redirecționate pentru colectare de date.

Detalii tehnice și modul de exploatare	❖ **Condiții necesare** • **Atacatorul trebuie să aibă acces la rețeaua în care dispozitivul este activ** pentru a trimite pachetele de date ce conțin comenzile injectate. • **Autentificare:** poate fi exploatată fără autentificare, ceea ce amplifică riscul de compromitere. ❖ **Exploatare** Vulnerabilitatea se manifestă prin faptul că dispozitivul vulnerabil execută comenzi nesecurizate, permițând atacatorilor să injecteze comenzi malefice la nivel de root. Un scenariu tipic de exploatare ar putea include: • **Identificarea dispozitivului Cisco vulnerabil** în rețea. • **Trimiterea unui pachet malițios** către dispozitiv, care conține comenzi arbitrare în formar de payload. • **Obținerea unui prompt cu privilegii root** care permit atacatorului să ruleze comenzi suplimentare la nivel de sistem. **Exemplu de Request Malițios (Simulat)** *"POST /vulnerable_endpoint HTTP/1.1* *Host: [IP-ul dispozitivului Cisco]* *Content-Type: application/x-www-form-urlencoded* *Content-Length: 100* *command=/bin/sh -c 'malicious_command' "*
Platforme de exploatare	❖ **Metasploit Framework** *"msfconsole* *use auxiliary/scanner/cisco/cisco_ios_auth_bypass # Exemplu pentru bypass autentificare Cisco* *set RHOSTS <IP-ul dispozitivului Cisco>* *run"* ❖ **Nmap și Nmap Scripting Engine (NSE)** *"nmap -sV --script=cisco-vuln-scripts -p <porturi_specifice> <IP-ul_dispozitivului>"* ❖ **Cisco Router and Switch exploitation Tool (Cisco-Torch)** *"cisco-torch -A -H <IP-ul_dispozitivului> -C config.txt -F brute_force.txt"* ❖ **Hydra (pentru forțarea autentificării)** *"hydra -l admin -P /path/to/password_list.txt <IP-ul_dispozitivului> ssh"*

	❖ **Python și resquests Library** *"import requests* *url = "http://<IP-ul_dispozitivului>/vulnerable_endpoint"* *payload = {'command': '/bin/sh -c "malicious_command"'}* *response = requests.post(url, data=payload)* *print(response.text)"* ❖ **Cisco Global Exploiter (CGE)** *"./cge.pl -t <IP-ul_dispozitivului> -p <port> -m <modul>"* ❖ **Telnet/SSH Clients** *"telnet <IP-ul_dispozitivului>* *# Sau pentru SSH* *ssh admin@<IP-ul_dispozitivului>"*
Recomandări de remediere	❖ **Actualizare software** • Accesați portalul Cisco pentru a descărca și instala cea mai recentă actualizare de firmware/software pentru dispozitiv. ❖ **Limitarea accesului de rețea** • Configurați firewall-ul pentru a restricționa accesul la dispozitiv doar din locațiile de rețea sigure. • Evitați expunerea dispozitivului direct către internet, utilizând segmente de rețea protejate. ❖ **Monitorizarea accesului** • Activați jurnalizarea detaliată (log-ing) și monitorizați log-urile pentru comenzi sau activități neobișnuite, care ar putea indica tentative de exploatare. • Implementați soluții de monitorizare pentru a detecta activitatea anormală a dispozitivelor Cisco. ❖ **Resetarea și revizuirea configurației** • După aplicarea patch-ului, revizuiți configurația dispozitivului pentru a vă asigura că nu există configurări care permit accesul nesecurizat. • Efectuați o resetare de securitate dacă suspectați că dispozitivul a fost compromis. ❖ **Restricții de acces pentru administrare** • Utilizați autentificarea multifactorială (MFA) pentru accesul administrativ și limitați numărul utilizatorilor care pot accesa interfața de administrare.

Măsuri suplimentare de protecție	Pentru a îmbunătăți securitatea dispozitivelor Cisco și a rețelei generale, vă recomandăm implementarea următoarelor măsuri suplimentare: 1. **Segmentarea rețelei**: Utilizați VLAN-uri și alte tehnici de segmentare pentru a izola dispozitivele Cisco de segmentele de rețea accesibile publicului sau mai puțin securizate. 2. **Autentificare și audit**: Asigurați-vă că doar utilizatorii autorizați au acces la configurațiile sensibile ale dispozitivului. Efectuați audituri periodice ale configurațiilor și log-urilor pentru a verifica integritatea dispozitivului. 3. **Monitorizarea traficului de rețea**: Utilizați IDS/IPS pentru a detecta și bloca traficul suspect care ar putea conține încercări de exploatare a acestei vulnerabilități. 4. **Educația și conștientizarea angajaților**: Asigurați-vă că echipa de administrare este informată cu privire la această vulnerabilitate și la măsurile de securitate. 5. **Plan de răspuns la incidente**: Dezvoltați un plan de răspuns rapid pentru incidente de securitate care vizează infrastructura Cisco.

Resurse externe

https://cybersecuritynews.com/cisco-flaw-attackers-command-root-user/