Raport consolidat eveniment cibernetic

CVE-2025-26465

Severitate	**Medie**
Modul de operare	Este o vulnerabilitate care a fost identificată în clientul OpenSSH (**versiunile 6.8p1 până la 9.9p1)** atunci când opțiunea **VerifyHostKeyDNS** este activată (setată ca: “yes” or “ask”). În aceste condiții există riscul de lansare a unui atac de tip machine-in-the-middle (MitM), prin care o mașină infectată se preface a fi un server legitim. Această problemă apare din cauza modului în care OpenSSH gestionează codurile de eroare în condiții specifice atunci când verifică cheia gazdă. **VerifyHostKeyDNS** este o opțiune de configurare a clientului OpenSSH care permite clientului SSH să caute și să verifice o cheie gazdă de tip serverthews utilizând înregistrări DNS (în special înregistrări SSHFP). Pentru ca un atac să fie considerat de succes, atacatorul trebuie să reușească să epuizeze mai întâi resursa de memorie a clientului, transformând complexitatea atacului.
Impactul potențial	• Interceptarea și manipularea sesiunilor SSH criptate. • Acces neautorizat la date și acreditări sensibile. • Mișcarea laterală potențială în cadrul rețelei dvs., ceea ce duce la compromiterea completă a sistemului.
Acțiuni recomandate	• Actualizează OpenSSH la versiunea 9.9p2, care corectează această vulnerabilitate, sau ulterioară. • Dezactivează opțiunea VerifyHostKeyDNS, dacă nu este absolut necesară în fișierele de configurare SSH globale și de utilizator. • Monitorizați-vă sistemele: Auditați periodic configurația SSH și jurnalele pentru orice semne de încercare de configurare greșită sau de intruziune.
	https://www.vicarius.io/vsociety/posts/cve-2025-26465-detect-vulnerable-openssh https://www.vicarius.io/vsociety/posts/cve-2025-26465-mitigate-vulnerable-openssh