Raport consolidat eveniment cibernetic

CVE-2024-41671

CVE-2024-41671 este o vulnerabilitate de tip **HTTP Request/Response Smuggling** care apare din cauza unei procesări incorecte a cererilor HTTP în cadrul serverului *twisted.web*.

Această vulnerabilitate poate duce la expunerea de informații între utilizatori sau la trimiterea de răspunsuri greșite către clienți. Problema este amplificată în mediile cu reverse proxy-uri, unde atacatorul poate exploata vulnerabilitatea pentru a manipula răspunsurile primite de alți clienți.

Informații suplimentare

TIP	**HTTP Request/Response Smuggling**
Versiunile afectate	twisted.web≤24.3.0
Instrumente de analiză	• Capturarea pachetelor *HTTP* cu ajutorul la *Wireshark*, cod pentru filtrarea pachetelor *HTTP Smuggling*: **“**http.request.line contains "Transfer-Encoding: chunked" and http.request.line contains "Content-Length"” • Detectarea cererilor *HTTP anormale* cu ajutorul al *Burp Suite* cu ajutorul comenzii: “Condition: Request header "Transfer-Encoding" present AND Request header "Content-Length" present Action: Log to console or alert” • Capturarea traficului de rețea cu ajutorul al *tcpdump* cu ajutorul comenzii: “sudo tcpdump -i any -A 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)'” • Testarea manuală a cererilor *HTTP* cu *curl și netcat*, prin intermediul codului: “(printf 'POST / HTTP/1.1\r\nTransfer-Encoding: chunked\r\n\r\n0\r\n\r\nPOST / HTTP/1.1\r\nContent-Length: 0\r\n\r\n'; sleep 1; printf 'GET / HTTP/1.1\r\n\r\n'; sleep 1) | nc localhost 80”
Condiții de exploatare	• Atacatorul trebuie să aibă capacitatea de a trimite cereri HTTP pipelate către serverul twisted.web. • Medii cu reverse *proxy-uri* și *pool-uri* de conexiuni măresc riscul de exploatare
Instrumente pentru efectuarea exploatării	• **netcat**: Utilizat pentru trimiterea cererilor HTTP pipelate. • **curl**: Utilizat pentru trimiterea cererilor HTTP complexe.

	• **Burp Suite Intruder**: Util pentru automatizarea trimiterii cererilor și observarea comportamentului anormal al serverului.
Impact	**Confidențialitate**: Atacatorul poate obține răspunsuri destinate altor utilizatori. **Integritate**: Răspunsurile pot fi alterate. **Disponibilitate**: Răspunsurile greșite pot destabiliza aplicația, dar nu cauzează oprirea completă.
Recomandări generice	• **Actualizarea framework-ului Twisted** la versiunea `24.7.0rc1` sau mai recentă pentru a rezolva problema de procesare a cererilor HTTP. • **Monitorizarea atentă a cererilor HTTP** pentru a detecta cererile pipelate anormale. • **Configurați proxy-urile și serverele back-end** să nu partajeze conexiuni între diferiți clienți, pentru a preveni exploatarea prin HTTP Request Smuggling.

Resurse externe

- https://github.com/twisted/twisted/commit/4a930de12fb67e88fefcb8822104152f42b27abc
- https://github.com/twisted/twisted/security/advisories/GHSA-c8m8-j448-xjx7
- https://nvd.nist.gov/vuln/detail/CVE-2024-41671