



Raport consolidat eveniment cibernetic

CVE-2024-42330

CVE-2024-42330 reprezintă o vulnerabilitate critică de tip execuție cod la distanță (RCE) identificată în platforma de monitorizare open-source Zabbix, cu un scor **CVSS 9.1**.

Vulnerabilitatea apare în modul de gestionare a antetelor HTTP în cadrul obiectului HttpRequest utilizat de Zabbix. Datele nesecurizate furnizate de server în antet sunt transformate în proprietăți ale obiectelor JavaScript fără o codificare adecvată. Această problemă permite unui atacator să:

- Trimite anteturi HTTP malițioase.
- Exploateze vulnerabilitatea pentru a accesa și manipula funcționalități interne ale serverului.
- Execute cod arbitrar pe serverele vulnerabile.

Informații suplimentare

Versiuni afectate	Următoarele versiuni ale Zabbix sunt vulnerabile: ✓ Zabbix 6.0.x ✓ Zabbix 6.4.x ✓ Zabbix 7.0.x
Vectorul de atac	❖ Vectorul de Atac: ✓ Scenariu: Un atacator trimite cereri HTTP concepute special către un server Zabbix configurat greșit sau expus public. ✓ Impact: Prin manipularea antetelor HTTP, atacatorul poate introduce cod arbitrar în serverele țintă. ❖ Cerințe pentru Exploatare:

	✓ Acces la rețea sau server Zabbix expus la internet. ✓ Lipsa unor controale de securitate suplimentare (autentificare strictă, firewall-uri configurate corect). Exemplu de exploatare: <pre>„POST /zabbix/api_jsonrpc.php HTTP/1.1 Host: victim-server User-Agent: custom Content-Type: application/json Content-Length: 150 Custom-Header: <script>alert('Exploited');</script> { "jsonrpc": "2.0", "method": "user.login", "params": { "user": "admin", "password": "zabbix" }, "id": 1}”</pre>
Impact asupra sistemului	❖ Preluarea Controlului: Execuția de cod malițios permite atacatorilor să controleze serverul complet. ❖ Propagare: Odată ce serverul este compromis, un atacator poate escalada atacul la alte sisteme din infrastructură. ❖ Compromiterea Datelor Sensibile: Zabbix este utilizat în medii critice și poate conține informații sensibile despre infrastructura monitorizată.
Soluții și măsuri de remediere	❖ Actualizări de securitate Zabbix a lansat patch-uri care remediază vulnerabilitatea în următoarele versiuni: • Zabbix 6.0.34rc1 • Zabbix 6.4.19rc1 • Zabbix 7.0.4rc1 ❖ Instrucțiuni pentru actualizare: ✓ Descărcați ultima versiune a software-ului de pe site-ul oficial Zabbix. ✓ Urmați documentația oficială pentru actualizare: „# Exemplu de actualizare pentru Debian/Ubuntu: <i>apt update</i> <i>apt upgrade zabbix-server-mysql zabbix-frontend-php zabbix-agent</i>”

	❖ Recomandări de securitate ✓ Restricționarea Accesului la Zabbix: • Permiteți accesul doar din rețelele de încredere. • Configurați firewall-uri pentru a bloca accesul la porturile Zabbix neautorizate. ✓ Activarea Autentificării Multi-Factor (MFA): • Asigurați conturile administrative cu autentificare suplimentară. ✓ Monitorizarea Activității Suspecte: • Configurați logurile pentru a înregistra și analiza cererile API suspecte. ✓ Revizuirea Configurațiilor Serverului: • Dezactivați funcționalitățile neutilizate sau expunerea API-urilor către internet. ✓ Testarea Vulnerabilității: • Rulați scanere de securitate pentru a verifica dacă serverul este vulnerabil.
Testare și validare	După aplicarea patch-urilor, efectuați următoarele verificări: • Test API: Verificați răspunsurile serverului pentru anteturi HTTP malițioase: <code>„curl -X POST http://your-zabbix-server/zabbix/api_jsonrpc.php \</code> <code>-H "Custom-Header: <script>alert('test');</script>" \</code> <code>-d '{"jsonrpc": "2.0", "method": "user.login", "params": {"user": "admin", "password": "test"}, "id": 1}'”</code> • Scanare de Securitate: Utilizați un scanner precum Nmap sau OpenVAS pentru a detecta vulnerabilități reziduale.

Resurse externe



<https://securityonline.info/cve-2024-42330-cvss-9-1-zabbix-patches-critical-remote-code-execution-vulnerability/>



<https://support.zabbix.com/browse/ZBX-12345>



<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-42330>