Zoom Workplace CVE 2025

Introducere	În 2025 au fost identificate mai multe vulnerabilități critice care afectează modul în care aplicațiile din ecosistemul **Zoom Workplace Apps** comunică prin intermediul WebSocket-urilor locale. Aceste vulnerabilități rezultă din absența unor mecanisme stricte de autentificare, validare a sursei și izolare a proceselor, permițând potențialilor atacatori să interacționeze neautorizat cu aplicațiile locale, să execute comenzi arbitrare sau să acceseze date sensibile. Exploatarea cu succes a acestor probleme poate compromite confidențialitatea, integritatea și securitatea generală a sesiunilor Zoom și a aplicațiilor integrate, afectând utilizatorii individuali cât și infrastructurile organizaționale.
Observabilitate și Instrumente de analiză	✓ Executa comenzi malițioase local sau de la distanță. ✓ Manipula fluxuri de date sau sesiuni fără cunoștința utilizatorului. ✓ Declanșa atacuri în lanț dintr-un simplu site compromis. ✓ Wireshark / mitmproxy - Inspectarea traficului WebSocket pe localhost ✓ Process Explorer- Identificarea aplicațiilor care deschid porturi locale ✓ Sysmon + SIEM (Splunk/ELK)- Detectarea conexiunilor neautorizate și scripturi automate ✓ Zoom logs- Monitorizarea comportamentului aplicațiilor Workplace
Detalierea CVE-urilor	
CVE-2025-27441 – Comenzi WebSocket neautorizate între aplicații	Permite unei aplicații *Zoom* instalate local să trimită comenzi către o altă aplicație, folosind conexiuni *WebSocket* partajate. **Mod de exploatare:** Atacatorul compromite o aplicație *Zoom* sau instalează una malițioasă. Aceasta deschide un canal *WebSocket* spre portul folosit de o aplicație legitimă și trimite comenzi în numele acesteia (ex: export date, inițiere acțiuni). • Comunicarea între aplicații *Zoom* se face prin *WebSocket JSON*, deschise pe porturi locale dinamic alocate (ex: ***127.0.0.1:3000-3999***). • Lipsa autentificării între instanțe permite unui client *WebSocket* să trimită comenzi precum: ***„{ "command": "triggerExport", "args": { "format": "CSV" } } ”*** • Comenzile nu sunt semnate sau validate cu *token* de sesiune → ușor de reprodus dintr-un script *JavaScript* local

CVE-2025-27442 – Injecție de cod prin canal WebSocket	Lipsa validării comenzilor în aplicațiile *Zoom* permite injecții de cod sau *payload*-uri malițioase transmise prin *WebSocket*. **Mod de exploatare :** Un atacator creează un script *JavaScript* sau o aplicație locală care inițiază o conexiune *WebSocket* către aplicația țintă și injectează comenzi prin mesaje *JSON* manipulate (ex:***{"command":"runScript","payload":"..."}).*** • Formatul mesajelor *JSON* transmis prin *WebSocket* permite inserarea de comenzi ofuscate (ex: base64, escape-uri): ***„ { "cmd": "runJS", "payload": "eval(String.fromCharCode(...))" } "*** • Aplicațiile vulnerabile nu filtrează caractere periculoase ***(<, >, ;, ")***, ceea ce deschide calea către injecții de cod *JavaScript* sau ***shell*** dacă sunt procesate cu ***eval(), new Function(),*** etc
CVE-2025-27443 – Acces nedorit între aplicații Zoom locale	Lipsa mecanismului de sandboxing permite accesul la resurse partajate de alte aplicații instalate în *Zoom Workplace*. **Mod de exploatare :** O aplicație malițioasă instalează un listener *WebSocket* sau inspectează porturi locale pentru a intercepta sesiuni active ale altor aplicații. • Aplicațiile *Zoom* funcționează în același context de proces sau container local, iar unele partajează fișiere temporare (***/tmp/zoomapp_shared.sock***), sockets sau storage comun (***IndexedDB***, ***localStorage***) Aceasta permite citirea/alterarea datelor salvate de alte aplicații, fără izolarea la nivel de UID/namespace
CVE-2025-30670 – Cross-Origin WebSocket Hijacking	Un site web malițios poate iniția conexiuni către aplicațiile *Zoom* locale, folosind *WebSocket*, fără ca ***Origin*** să fie verificat. **Mod de exploatare:** Utilizatorul accesează un site compromis. Acesta deschide un *WebSocket* către ***ws://localhost:<port>*** și trimite comenzi către aplicația *Zoom* activă, preluând controlul asupra funcțiilor acesteia. • Atacatorul poate deschide dintr-o pagină web un WebSocket către: „const socket = new WebSocket("ws://localhost:3498"); socket.onopen = () => socket.send(JSON.stringify({ action: "startRecording" })); " • Deoarece aplicația Zoom nu verifică *Origin* header, acest mesaj este acceptat → deturnarea funcției.
CVE-2025-30671 – Lipsă autentificare pe porturile locale	Porturile *WebSocket* deschise de aplicațiile *Zoom* nu verifică identitatea entităților care le accesează. **Mod de exploatare:**

	Un atacator execută un script local (din browser, terminal sau aplicație Electron) care comunică cu portul local deschis de Zoom și execută funcții fără autentificare (ex: trimite date, generează acțiuni). • Lipsa unui mecanism de ***CSRF token,*** semnătură *HMAC*, sau ***TLS*** mutual pe canalul *WS* permite ca orice aplicație locală să trimită comenzi direct în APIul Zoom App Porturile locale sunt de tip ***ws://127.0.0.1:<dynamic>*** fără whitelisting de proces/UID
CVE-2025-30672 – Comenzi arbitrare prin WebSocket fără sesiune validă	Aplicațiile *Zoom* acceptă comenzi de la clienți *WebSocket* care nu au sesiune validă sau token de autentificare. **Mod de exploatare:** Un script din browser sau aplicație locală deschide un canal *WS* către aplicația Zoom și trimite comenzi predefinite (ex: openMeeting, sendMessage), fără a fi parte dintr-o sesiune autorizată. • Comenzile WebSocket acceptă ***sessionId***, ***userContext***, ***appId***, dar aceste valori sunt presetate la valori default sau absente. • Exemplu de comandă validă fără sesiune reală: „{ "appId": "crmApp", "command": "fetchContacts" } ” • Fără validarea sesiunii/semnăturii, comanda este executată imediat → exploatare facilă.
Redomandări	✓ Verificare versiune Zoom pe toate endpointurile. ✓ Dezinstalarea aplicațiilor Zoom necunoscute sau nevalidate. ✓ Blocarea porturilor locale neutilizate (WS) și activare EDR. ✓ Notificare utilizatorilor despre update-ul de securitate.
Referințe	https://cybersecuritynews.com/zoom-workplace-apps-vulnerability/ https://www.zoom.com/en/trust/security-bulletin/