Vulnerabilități Ridicat
Microsoft Office CVE-2026-21509

CVSS	7.8 (RIDICAT)
Tipul Vulnerabilității	Bypass al caracteristicii de securitate din Microsoft Office (security-feature bypass).
Mod de exploatare	Atac local care necesită interacțiunea utilizatorului; atacatorul trimite un fișier Office special creat și convinge victima să îl deschidă.
Cauza	Aplicația se bazează pe intrări neîncredibile când ia decizii de securitate, permițând ocolirea mitigărilor OLE (Object Linking and Embedding) destinate protejării împotriva controlurilor vulnerabile COM/OLE.
Metoda de Exploatare	• Distribuire inițială (phishing) E-mailuri țintite livrează documente Word/RTF malițioase ce conțin exploit pentru CVE-2026-21509. • Declanșare exploit (deschiderea fișierului) Office ocolește protecțiile OLE/COM și inițiază automat conexiune WebDAV către serverul atacatorului. • Dropper local Se descarcă un fișier .LNK, care execută cod și instalează: – EhStoreShell.dll (DLL malițios) – SplashScreen.png (shellcode ascuns) • Persistență (COM hijacking) Modifică registry (CLSID hijack) + creează task programat OneDriveHealth pentru execuție automată la fiecare pornire. • Control la distanță (C2) Se lansează implantul Covenant (.NET), comunicând cu infrastructura C2 prin Filen.io pentru mascarea traficului. • Payload-uri suplimentare (opțional) Posibilă instalare de stealere/backdoor-uri (ex. MiniDoor, loadere personalizate).
Versiuni Afectate	Office 2016, Office 2019, Office LTSC 2021, Office LTSC 2024, Microsoft 365 Apps for Enterprise
Consecințe	Bypass-ul permite încărcarea neautorizată a unor componente COM și executarea de cod malițios, compromițând confidențialitatea, integritatea și disponibilitatea sistemului
Detectare și monitorizare	• Supravegherea rețelei: Blocați sau monitorizați conexiunile către domeniile și IP-urile asociate serviciului Filen.io și altor infrastructuri identificate de CERT-UA. Monitorizați traficul WebDAV neobișnuit. • Detecții de COM hijacking: Căutați în registru CLSID-uri modificate (de ex. {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D} și {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}) și fișierele EhStoreShell.dll și SplashScreen.png în locațiile de sistem. • Scanare pentru Covenant/MiniDoor: Folosiți instrumente EDR/AV cu semnături pentru Covenant Grunt (C2) și pentru dropperele PixyNetLoader sau MiniDoor. • Training anti-phishing: Dat fiind că atacul necesită interacțiunea utilizatorului, educarea personalului privind recunoașterea emailurilor suspecte este esențială.