Raport consolidat eveniment cibernetic

Informații suplimentare

Denumire	**CVE-2024-21413**
Tip	Microsoft Outlook Remote Code Execution Vulnerability
Descriera	• Cauza principală a acestei vulnerabilități provine din interpretarea greșită unor linkuri **hipertext** de către Office, în special a linkurilor care se bazează pe tehnologia **COM Monikers** (această tehnologie permit aplicațiilor să acceseze și să gestioneze în mod uniform obiecte, făcându-le integrale, dar potențial periculoase). • Dacă această legătură indică spre o partajare SMB – în formularul \\<**Malicious_IP**>\fișier – apoi programul Office va încerca automat să se autentifice pe acest server de la distanță prin trimiterea unui **NTLM hash** al utilizatorului curent. Dacă acest server SMB trimite un fișier rău intenționat ca un **RTF**, atunci Microsoft Word va încărca fișierul.
Detalii vulneabilitate	1. **Atac Vector:** Defecțiunea, numită Moniker Link, permite atacatorilor să ocolească protecția încorporată în Outlook pentru link-urile rău intenționate încorporate în e-mailuri. 2. **Protected View Bypass:** Atacatorii pot ocoli Office Protected View, conceput pentru a bloca conținutul dăunător prin deschiderea fișierelor în modul doar în modul citire, permițându-le să deschidă fișiere Office rău intenționate în modul de editare. 3. **Previzualizare Pane Exploatare:** Panoul de previzualizare din Outlook servește ca vector de atac suplimentar, permițând exploatarea chiar și atunci când previzualizați documente Office rău intenționate. 4. **NTLM Credential Leak:** Exploatarea cu succes a CVE-2024-21413 poate duce la furtul informațiilor de acreditare NTLM, acordând atacatorilor privilegii ridicate, inclusiv citirea, scrierea și ștergerea funcționalității.

MITRE ATT&CK techniques	T1566.002 - Phishing: Spearphishing Link T1559.001 - Inter-Process Communication T1204.001 - User Execution: Malicious Link
Produsele afectate	Microsoft Office 2016 Microsoft Office 2019 Microsoft Office 2021 Microsoft 365 Apps
Recomandări	• **Aplicare Patch oficial:** Microsoft a lansat un patch de securitate care se adresează CVE-2024-21413. Toți utilizatorii Outlook sunt sfătuiți să aplice imediat patch-ul oficial. • **Actualizați software-ul:** Asigurați-vă că Microsoft Office, inclusiv Outlook, este actualizat în mod regulat la cea mai recentă versiune pentru a beneficia de îmbunătățiri de securitate și remedieri de erori. • **Atenție la email-uri:** Exercitați prudență la deschiderea e-mailurilor, în special a celor din surse necunoscute sau neîncrezătoare. Fiți atenți la e-mailurile care conțin linkuri sau atașamente. • **Blocare port:** Dacă actualizarea nu este posibilă, pentru a atenua impactul acestei vulnerabilități este necesar blocarea traficului de ieșire pe portul **445**.