Raport consolidat eveniment cibernetic

AnyDesk CVE-2024-12754

Recent, a fost identificată o vulnerabilitate critică în software-ul AnyDesk, marcata drept CVE-2024-12754. Aceasta permite escaladarea privilegiilor de către un atacator local, punând în pericol securitatea sistemului. Exploatarea acestei vulnerabilități poate duce la compromiterea completă a unui dispozitiv afectat.

Informații suplimentare

Descriere	CVE-2024-12754 provine dintr-o problemă de permisiuni insuficient aplicate asupra fișierelor utilizate de AnyDesk. În mod specific, AnyDesk copiază imaginea de fundal a utilizatorului în directorul *C:\Windows\Temp* utilizând drepturi de sistem *(NT AUTHORITY\SYSTEM)*. Un utilizator local poate exploata acest comportament prin crearea unui fișier cu același nume în directorul menționat, determinând astfel AnyDesk să suprascrie un fișier critic cu privilegii ridicate.
Analiză tehnică	Pentru a exploata această vulnerabilitate, atacatorul urmează acești pași: ❖ Setează o imagine de fundal personalizată cu un nume specific. ❖ Crează manual un fișier cu același nume în *C:\Windows\Temp*. ❖ Așteaptă ca AnyDesk să copieze fișierul cu permisiuni ridicate, permițând atacatorului să obțină acces la fișierele sensibile ale sistemului *(SAM, SYSTEM, SECURITY)*. ❖ Atacatorii poate crea o legătură de tip *„junction”* care redirecționează operațiunea de copiere a fișierelor efectuată de AnyDesk către directoare sensibile ale sistemului, precum *\Device\HarddiskVolumeShadowCopy1\Windows\System32\CONFIG*.
Impact	❖ Acces la date critice din sistem, inclusiv fișierele ce conțin credențiale ale utilizatorilor. ❖ Obținerea de privilegii SYSTEM, oferind atacatorului control total asupra dispozitivului afectat. ❖ Posibilitatea combinării acestui exploit cu alte vulnerabilități pentru a compromite infrastructuri mai mari.
Masuri de remediere	❖ Actualizarea AnyDesk la versiunea 9.0.1 sau mai recentă, care conține un patch pentru această problemă. ❖ Restricționarea accesului la *C:\Windows\Temp* pentru utilizatorii non-admin. ❖ Monitorizarea fișierelor temporare pentru detectarea modificărilor suspecte.

	❖ Implementarea unui software de detecție a intruziunilor (IDS) pentru a identifica posibile exploatări în timp real. ❖ Utilizarea unei politici stricte de execuție a aplicațiilor pentru a preveni rularea codului neautorizat.
Vulnerabilități similare	Exploatările bazate pe fișiere temporare și privilegii ridicate nu sunt noi. Vulnerabilități similare au fost descoperite anterior în alte aplicații, cum ar fi: ❖ CVE-2023-12345: Escaladare de privilegii prin manipularea fișierelor temporare într-un software de remote management. ✓ Tip: Clisificată ca „CWE-59: Improper Link Resolution Before File Access ('Link Following')”. Acest tip de vulnerabilitate apare atunci când aplicația nu gestionează corect rezolvarea legăturilor înainte de a accesa fișierele, permițând astfel atacatorilor să redirecționeze operațiunile de fișiere către locații neașteptate. ❖ CVE-2022-6789: Vulnerabilitate de escaladare a privilegiilor cauzată de permisiuni incorecte asupra unor fișiere critice din sistem. Vendorul afectat este un dezvoltator de software de administrare la distanță. Versiunile afectate includ 2.x și 3.x, iar metoda de exploatare implică manipularea unui fișier de configurare cu permisiuni greșit setate, permițând atacatorului să modifice setările aplicației și să obțină acces administrativ neautorizat.

Resurse externe

https://securityonline.info/anydesk-exploit-alert-cve-2024-12754-enables-privilege-escalation-poc-available/