CTI Riport

Egy a Microsoft Exchange szervert érintő magas súlyosságú sérülékenységről

2025. augusztus 15.

Tartalom

Összefoglalás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Kiberfenyegetettség elemző főosztálya rendszeresen végez elemzéseket a hozzá beérkező, harmadik féltől származó információk, valamint saját kutatásai alapján. Az alábbi riport egy, a Microsoft Exchange szervert érintő, magas súlyosságú sérülékenységre hívja fel a figyelmet, és haladéktalanul javasolja a szükséges frissítések telepítését. A sérülékenység kihasználása lehetővé teheti illetéktelen hozzáférést és jogosultságkiterjesztést a rendszerben, ezért a frissítési folyamat elvégzése kiemelten fontos a szervezet adatainak és levelezési infrastruktúrájának védelme érdekében.

2025. április 18-án a Microsoft bejelentette a Microsoft Exchange Server hibrid telepítéseit érintő biztonsági változtatásokat, valamint egy ehhez kapcsolódó, nem biztonsági jellegű hotfix frissítést. A Microsoft ezeket a módosításokat általános biztonsági szempontok érdekében hajtotta végre, a hibrid Exchange környezetek védelmének javítása céljából.

A későbbi, részletesebb vizsgálatok során a Microsoft azonosított olyan konkrét biztonsági vonatkozásokat, amelyek közvetlenül kapcsolódnak a 2025. áprilisi bejelentésben leírt útmutatásokhoz és konfigurációs lépésekhez.

Ennek eredményeként a Microsoft kiadta a CVE-2025-53786 azonosítót, amely hivatalosan dokumentálja azt a sérülékenységet, amely a 2025. április 18-i bejelentésben ismertetett lépések végrehajtásával megszüntethető.

A Microsoft nyomatékosan javasolja:

- Az április 2025-ös (vagy újabb) hotfix telepítését
- A közzétett konfigurációs változtatások teljes körű bevezetését mind az Exchange Server, mind a hibrid környezet beállításaiban.

A CVE-2025-53786 sérülékenység

A sérülékenység leírása, hatása

2025. augusztus 6-án a Microsoft biztonsági figyelmeztetést adott ki egy magas súlyosságú sérülékenységgel kapcsolatban, amely elsősorban a Microsoft Exchange hibrid környezeteket érinti (Exchange Server 2016, Exchange Server 2019 és Exchange Server Subscription Edition). Ez a kockázat abból adódik, hogy a hibrid konfigurációban az Exchange Server és az Exchange Online ugyanazt a service principal azonosítót használja, amely egy alkalmazás vagy szolgáltatás identitása az Azure AD-ban, ami hitelesítésre és engedélyezésre szolgál.

A CVE-2025-53786 azonosítón nyilvántartott sérülékenység lehetővé teszi, hogy egy, a helyszíni (on-premises) Exchange szerverhez adminisztrátori hozzáféréssel rendelkező támadó jogosultság eszkalációt hajtson végre a kapcsolódó Exchange Online környezetben (e-mail, naptár, fiókkezelési funkciók) úgy, hogy nem hagy könnyen észlelhető vagy naplózható nyomot maga mögött. A sérülékenység sikeres kihasználásához a támadónak először adminisztrátori hozzáférést kell szereznie az Exchange Serveren, tehát nem használható ki közvetlenül, belépési jogosultság nélkül.

A sérülékenység hatással lehet az érintett rendszerek bizalmasságára, sértetlenségére és rendelkezésre állására.

Egy, a helyszíni Exchange szerveren adminisztrátori jogosultságokkal rendelkező támadó képes lehet hamisítani vagy manipulálni olyan megbízhatónak tekintett tokeneket, illetve API-hívásokat, amelyeket a felhőoldali rendszer érvényesnek fogad el. Ez a technika lehetővé teszi, hogy a támadó oldalirányban (lateral movement) terjedjen az on-premises környezetből (helyi hálózatból) a szervezet felhőalapú környezetébe, potenciálisan veszélyeztetve a szervezet teljes Active Directory-ját és infrastruktúráját. Ezzel a hibrid identitásmodell gyengeségeit kihasználva a támadó átveheti az irányítást a teljes tartomány felett.

Összegezve, a támadó, ha adminisztrátori jogosultságot szerez az on-premises Exchange szerveren, képes:

- Hamisított vagy manipulált bizalmi tokenek (trusted token) előállítására
- API-hívások manipulálására az Azure AD irányába
- A felhőszolgáltatásban magasabb jogosultságok megszerzésére
- Nyommentes privilégium eszkalációra, ami jelentősen nehezíti a detektálást

Ez a magas kockázatú sérülékenység minden olyan szervezetet érint, amely Microsoft Exchange hibrid konfigurációt üzemeltet és nem hajtotta végre a 2025. áprilisi biztonsági frissítéseket (1. ábra).

A Microsoft intézkedései

A sérülékenységet a Microsoft 2025 áprilisában hozta nyilvánosságra, egy hotfix és egy részletes mitigációs útmutató kíséretében.

A javítás része a Secure Future Initiative-nek, amely új architektúrát vezet be:

- A régi shared identity modell lecserélése
- Egy dedikált hibrid alkalmazás bevezetése a biztonságos kommunikáció érdekében az on-premises Exchange és az Exchange Online között

A Microsoft a sérülékenységet „Exploitation More Likely” besorolással látta el, ami azt jelzi, hogy várhatóan exploit kód jelenhet meg, jelentősen növelve a támadás kockázatát.

Érintett rendszerek

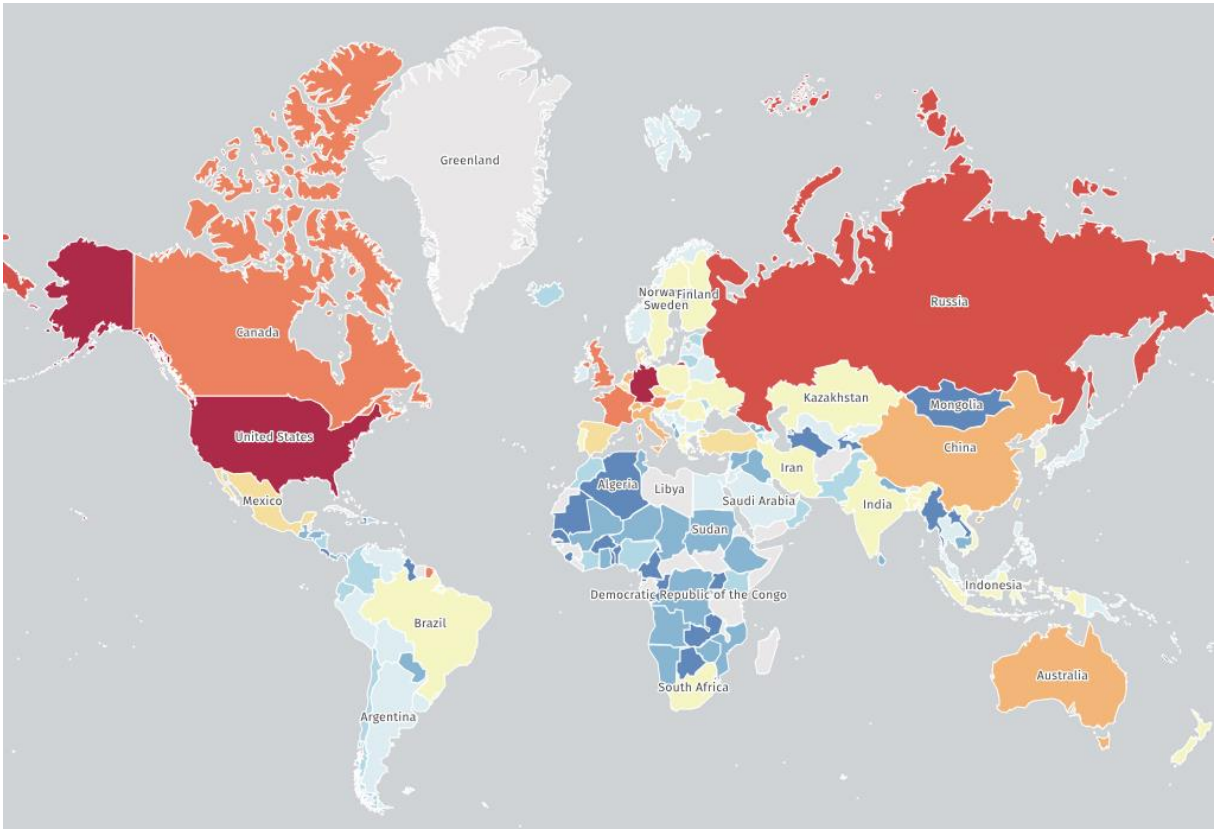
A sérülékenység az alábbi, hibrid Exchange környezetben üzemelő Microsoft Exchange Server-verziókat érinti:

- Microsoft Exchange Server 2016 Cumulative Update 23 15.01.2507.055 verziójánál korábbi verziókat
- Microsoft Exchange Server 2019 Cumulative Update 14 15.02.1544.025 verziójánál korábbi verziókat
- Microsoft Exchange Server 2019 Cumulative Update 15 15.02.1748.024 verziójánál korábbi verziókat

- Microsoft Exchange Server Subscription Edition RTM 15.02.2562.017 verziójánál korábbi verziókat

Shadowserver adatok

A Shadowserver 2025. augusztus 10-i szkennelése szerint 29 098 szerver maradt frissítetlen, az Egyesült Államokban körülbelül 7 200 IP Németországban 6 700, Oroszországban 2 500. Ez a kitettség jelentős támadási felületet kínál a potenciális fenyegető szereplőknek.



1. ábra Támadásnak kitett Microsoft Exchange szerverek forrás: Shadowserver

Kormányzati szervek - kötelező mitigáció

Az amerikai Cybersecurity and Infrastructure Security Agency (röviden: CISA) a sérülékenység publikálását követően 2025. augusztus 7-én adta ki az Emergency

Directive 25-02 (röviden: ED 25-02) direktívát, amelyben arra kötelezi az amerikai szövetségi ügynökségeket, hogy kezeljék a hibát. A direktíva értelmében minden érintett ügynökségnek 2025. augusztus 11-én, 9:00 AM EDT-ig kell végrehajtania a kötelező intézkedéseket. A direktíva mindaddig érvényben marad, amíg CISA nem tekinti lezártnak az intézkedések foganatosítását, vagy azt más hivatalos eljárás keretébe visszavonásra nem kerül.

Előírt lépések:

1. Exchange környezet felmérése – Microsoft Health Checker script használatával
2. Nem támogatott verziók azonnali leválasztása az internetről (EOL/EOS állapotú rendszerek)
3. Frissítés a legújabb kumulatív csomagra (CU14/CU15 – Exchange 2019, CU23 – Exchange 2016)
4. Áprilisi hotfix telepítése

A CISA figyelmeztetése szerint a hiba figyelmen kívül hagyása hibrid és on-premises környezet teljes kompromittálását okozhatja.

Nem kormányzati szervek – sürgős ajánlás

Bár a direktíva jogilag nem kötelezi a magán- és civil szervezeteket, a CISA nyomatékosan ajánlja ugyanazon intézkedések végrehajtását. A kockázat ugyanis minden Exchange-alapú hibrid környezetben fennáll, függetlenül az iparágtól vagy a szervezet típusától.

Magyarországi érintettség

A rendelkezésre álló információk alapján megállapítható, hogy a sérülékenységnek Magyarországon is van érintettsége.

- Magyarországi érintettek száma: 306 darab
- Ebből kormányzati szereplők (gov.hu tartomány): 15 darab
- Nem kormányzati érintettség: 291 darab

Összegzés

A CVE-2025-53786 sebezhetőség nemcsak a kormányzati szektort fenyegeti, hanem minden Microsoft Exchange-t használó szervezetet. A javítás halogatása jelentősen megnöveli egy **teljes tartománykompromittálás** kockázatát, ezért a **frissítések azonnali telepítése** kulcsfontosságú.

Az NBSZ-NKI által javasolt intézkedések

1. Exchange szerverek azonosítása és állapotuk felmérése

Az azonosítás célja, hogy teljes listát kapjunk az aktív on-premises Exchange példányokról. Javasolt, a Microsoft Exchange Server Health Checker script lefuttatása a szerverek állapotának feltérképezésére.

2. Elavult/hibás szerverek lekapcsolása

Azokat a szervereket, amelyek nem jogosultak az április 2025-ös Hotfix frissítésre, különösen az elavult, end-of-life példányokat, javasolt lekapcsolni a hálózatról.

3. Frissítés a megfelelő CU szintre és hotfix telepítése

A megmaradt, jogosult szervereket a legfrissebb Cumulative Update verzióra szükséges frissíteni (az Exchange 2019-et CU14, vagy CU15 -re, az Exchange 2016-ot CU23-ra). Ezt követően pedig telepíteni kell a Microsoft 2025. áprilisi Exchange Server Hotfix frissítéseit a helyszíni (on-premise) Exchange szerverre, majd pedig a Microsoft konfigurációs utasításai alapján a dedikált Exchange hibrid alkalmazást.

4. Service Principal elválasztása

Olyan szervezetek esetén, amelyek dedikált Exchange Hybrid alkalmazást használnak, vagy korábban konfiguráltak, de már nem használják, javasolt a service principal objektum keyCredentials értékeinek visszaállítása a Microsoft Service Principal Clean-Up Mode útmutatója szerint.

5. Monitorozás

Javasolt a hibrid hitelesítési események és anomáliák folyamatos figyelése. A frissítés után legalább 72 órás aktív logfigyelés ajánlott.

Kérjük, amennyiben a vizsgálattal összefüggően további kérése merül fel, illetve a monitorozott technikai azonosítókban hibát, vagy hiányosságot fedezett fel, értesítse intézetünket a cyberthreat@nki.gov.hu, CSIRT@nki.gov.hu címen, vagy ezen dokumentumot tartalmazó üzenetre adott válasz formájában.

Nemzetbiztonsági Szakszolgálat

Nemzeti Kiberbiztonsági Intézet