



**TLP: CLEAR**

**Szabadon terjeszthető!**

## Riasztás

### Microsoft termékeket érintő sérülékenységekről

(2024. február 14.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki a **Microsoft** szoftvereket érintő **kritikus kockázati besorolású** sérülékenységek kapcsán, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft 2024. február havi biztonsági csomagjában összesen **73** különböző **biztonsági hibát javított**, köztük **5 kritikus** kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kód futtatást, szolgáltatásmegtagadást, jogosulatlan adathozzáférést és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren. A javított sérülékenységek között **2 db nulladik napi (zero-day)** sebezhetőség található.

[CVE-2024-21351](#) - Windows SmartScreen Security Feature Bypass Vulnerability

[CVE-2024-21412](#) - Internet Shortcut Files Security Feature Bypass Vulnerability

**A sebezhetőségek patchelése **MAGAS** prioritású, mivel adathalász technikával (e-mail csatolmány segítségével) felhasználható káros kóddal történő fertőzésre.**

A Trend Micro [biztonsági közleménye](#) szerint legalább egy **APT** csoport (**DarkCasino (Water Hydra)**) aktívan ki is használta a sebezhetőségeket a **DarkMe** elnevezésű káros kód terjesztésére.

**Érintett termékek és szerepkörök:** Microsoft Office, Azure Stack, Windows Hyper-V, Skype for Business, Trusted Compute Base, Microsoft Defender for Endpoint, Microsoft Dynamics, Azure Connected Machine Agent, Windows Kernel, Windows USB Serial Driver, Role: DNS Server, Windows Internet Connection Sharing (ICS), Windows Win32K – ICOMP, SQL Server, Microsoft ActiveX, Microsoft WDAC OLE DB provider for SQL, Windows SmartScreen, Microsoft WDAC ODBC Driver, Windows Message Queuing, Windows LDAP - Lightweight Directory Access Protocol, Azure Site Recovery, Windows OLE, Microsoft Teams for Android, Microsoft Azure Kubernetes Service, Microsoft Windows DNS, Microsoft Office Outlook, Microsoft Office Word, Azure Active Directory, Microsoft Office OneNote, .NET, Azure File Sync, Microsoft Edge (Chromium-based), Microsoft Windows, Microsoft Exchange Server, Internet Shortcut Files

**TLP: CLEAR**



**TLP: CLEAR**

Szabadon terjeszhető!

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.

Hivatkozások:

- <https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2024-patch-tuesday-fixes-2-zero-days-74-flaws/>
- [https://www.trendmicro.com/en\\_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html](https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html)

Nemzetbiztonsági Szakszolgálat  
Nemzeti Kibervédelmi Intézet  
Telefon: +36-1-336-4833  
Incidensbejelentés: [csirt@nki.gov.hu](mailto:csirt@nki.gov.hu)

NEMZETI  
KIBERVÉDELMI INTÉZET

**TLP: CLEAR**