

Riasztás

Microsoft termékeket érintő sérülékenységekről

(2023. április 13.)

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 2023. április havi biztonsági csomagjában összesen **97** különböző **biztonsági hibát javított**, köztük **7 kritikus** kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kód futtatást, szolgáltatásmegtagadást és jogosultság kiterjesztést tesznek lehetővé a sérülékeny rendszeren. A javított sérülékenységek között **egy nulladik napi (zero-day)** sebezhetőség is található:

- [CVE-2023-28252](#) (Windows Common Log File System Driver Elevation of Privilege Vulnerability)

Érintett termékek és szerepkörök: .NET Core, Azure Machine Learning, Azure Service Connector, Microsoft Bluetooth Driver, Microsoft Defender for Endpoint, Microsoft Dynamics, Microsoft Dynamics 365 Customer Voice, Microsoft Edge, Microsoft Graphics Component, Microsoft Message Queuing, Microsoft Office, Microsoft Office Publisher, Microsoft Office SharePoint, Microsoft Office Word, Microsoft PostScript Printer Driver, Microsoft WDAC OLE DB provider for SQL, Microsoft Windows DNS, Visual Studio, Visual Studio Code, Windows Active Directory, Windows ALPC, Windows Ancillary Function Driver for WinSock, Windows Boot Manager, Windows Clip Service, Windows CNG Key Isolation Service, Windows Common Log File System Driver, Windows DHCP Server, Windows Enroll Engine, Windows Error Reporting, Windows Group Policy, Windows Internet Key Exchange Protocol, Windows Kerberos, Windows Kernel, Windows Layer 2 Tunneling Protocol, Windows Lock Screen, Windows Netlogon, Windows Network Address Translation, Windows Network File System, Windows Network Load Balancing, Windows NTLM, Windows PGM, Windows Point-to-Point Protocol over Ethernet, Windows Point-to-Point Tunneling Protocol, Windows Raw Image Extension, Windows RDP Client, Windows Registry, Windows RPC API, Windows Secure Boot, Windows Secure Channel, Windows Windows Secure Socket Tunneling Protocol, Windows Transport Security Layer, Windows Win32K

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

Hivatkozások:

- <https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2023-patch-tuesday-fixes-1-zero-day-97-flaws/>
- <https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr>

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