TLP:WHITE
Szabadon terjeszthető!

Riasztás
Microsoft termékeket érintő sérülékenységekről

(2022. október 12.)

Tisztelt Ügyfelünk!

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

A Microsoft 2022. október havi biztonsági csomagjában összesen **84** különböző biztonsági hibát javított, köztük **13** „kritikus" besorolású, mivel távoli kódfuttatást vagy jogosultság kiterjesztést tesznek lehetővé. Ezek közül kiemelendő a SharePoint szerverek sérülékenysége (CVE-2022-41038), amelyről feltételezhető, hogy azt fenyegetési szereplők megpróbálják kihasználni.

A javított sérülékenységek között **kettő nulladik napi (zero-day)** hiba is található. Ezek közül az első, CVE-2022-41033 számon nyilvántartott sebezhetőség segítségével rendszerszintű hozzáférés szerezhető, a Microsoft pedig arra figyelmezet, hogy ezt támadók már **aktívan kihasználják**.

Az Exchange szerverek korábban nyilvánosságra hozott „ProxyNotShell" sebezhetőségeihez (CVE-2022-41040 és a CVE-2022-41082) azonban továbbra sem jelent meg javítás, ezért a javasolt gyártói mitigáció alkalmazása.

Érintett termékek és szerepkörök: Active Directory Domain Services, Azure, Azure Arc, Client Server Run-time Subsystem (CSRSS), Microsoft Edge (Chromium-based), Microsoft Graphics Component, Microsoft Office, Microsoft Office SharePoint, Microsoft Office Word, Microsoft WDAC OLE DB provider for SQL NuGet Client, Remote Access Service Point-to-Point Tunneling Protocol, Role: Windows Hyper-V, Service Fabric, Visual Studio Code, Windows Active Directory Certificate Services, Windows ALPC, Windows CD-ROM Driver, Windows COM+ Event System Service, Windows Connected User Experiences and Telemetry, Windows CryptoAPI, Windows Defender, Windows DHCP Client, Windows Distributed File System (DFS), Windows DWM Core Library, Windows Event Logging Service, Windows Group Policy, Windows Group Policy Preference Client, Windows Internet Key Exchange (IKE) Protocol, Windows Kernel, Windows Local Security Authority (LSA), Windows Local Security Authority Subsystem Service (LSASS), Windows Local Session Manager (LSM), Windows NTFS, Windows NTLM, Windows ODBC Driver, Windows Perception Simulation Service, Windows Point-to-Point Tunneling Protocol, Windows Portable Device Enumerator Service, Windows Print Spooler Components, Windows Resilient File System (ReFS), Windows Secure Channel, Windows Security Support Provider Interface, Windows Server Remotely Accessible Registry Keys, Windows Server Service, Windows Storage, Windows TCP/IP, Windows USB Serial Driver, Windows Web Account Manager, Windows Win32K, Windows WLAN Service, Windows Workstation Service

TLP:WHITE
Szabadon terjeszthető!

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

Hivatkozások:

- **https://www.cisa.gov/uscert/ncas/current-activity/2022/10/11/microsoft-releases-october-2022-security-updates**
- **https://msrc.microsoft.com/update-guide/releaseNote/2022-Oct**
- **https://blog.talosintelligence.com/2022/10/microsoft-patch-tuesday-for-october.html**
- **https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2022-patch-tuesday-fixes-zero-day-used-in-attacks-84-flaws/**

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