TLP:WHITE
Szabadon terjeszthető!

Riasztás
Microsoft termékeket érintő sérülékenységekről

(2023. március 16.)

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 2023. március havi biztonsági csomagjában összesen **83** különböző biztonsági hibát javított, köztük **7 kritikus** kockázati besorolású, amelyek sikeres kihasználása többek között szolgáltatásmegtagadást, jogosultságnövelést, illetve távoli kódfuttatást tehet lehetővé.

A javított sérülékenységek között **két nulladik napi (zero-day)** sebezhetőség is megtalálható, amelyeket az Egyesült Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökségének (CISA) jelzése szerint fenyegetési szereplők **aktívan ki is használnak**:

- **Microsoft Outlook sérülékenysége (CVE-2023-23397, CVSS 3.1 pontszám: 9.8)**
- **Windows SmartScreen sérülékenysége (CVE-2023-24880, CVSS:3.1 pontszám: 5.4)**

Az Outlookot érintő sérülékenység kapcsán a Microsoft egy külön tájékoztatóban bővebb információval szolgál a hiba kihasználásáról, emellett egy szkriptet is közreadott, amely Exchange rendszerüzemeltetők számára segítséget nyújt annak megállapításához, hogy rendszerük érintett-e a sérülékenységet kihasználó támadásban. A CERT-EU a szkript alkalmazásakor első lépésben az „audit mode" használatát javasolja az esetleges digitális nyomok megőrzése érdekében, illetve megelőző intézkedésként az SMB hálózati szolgáltatás által használt TCP 445 port tiltását az Internet irányából.

Érintett termékek és szerepkörök:

Azure, Client Server Run-time Subsystem (CSRSS), Internet Control Message Protocol (ICMP), Mariner, Microsoft Bluetooth Driver, Microsoft Dynamics, Microsoft Edge (Chromium-based), Microsoft Graphics Component, Microsoft Office Excel, Microsoft Office Outlook, Microsoft Office SharePoint, Microsoft OneDrive, Microsoft PostScript Printer Driver, Microsoft Printer Drivers, Microsoft Windows Codecs Library, Office for Android, Remote Access Service Point- to-Point Tunneling Protocol, Role: DNS Server, Role: Windows Hyper-V, Service Fabric, Visual Studio, Windows Accounts Control, Windows Bluetooth Service, Windows Central Resource Manager, Windows Cryptographic Services, Windows Defender, Windows http Protocol Stack, Windows HTTP.sys, Windows Internet Key Exchange (IKE) Protocol, Windows Kernel, Windows Partition Management Driver, Windows Point-to-Point Protocol over Ethernet (PPPoE), Windows Remote Procedure Call, Windows Remote Procedure Call Runtime, Windows Resilient File System (ReFS), Windows Secure Channel, Windows SmartScreen, Windows TPM, Windows Win32K

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

TLP:WHITE
Szabadon terjeszthető!

Hivatkozások:

- https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24880
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23397
- https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/
- https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/
- https://www.cert.europa.eu/static/SecurityAdvisories/2023/CERT-EU-SA2023-018.pdf
- https://www.cisa.gov/news-events/alerts/2023/03/14/cisa-adds-three-known-exploited-vulnerabilities-catalog

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