

TLP:WHITE

Szabadon terjeszhető!

Rendkívüli tájékoztatás

Microsoft Windows Support Diagnostic Tool (MSDT) zero-day sérülékenység kapcsán

(2022. június 01.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **tájékoztatást** ad ki a Microsoft Windows Support Diagnostic Toolt (MSDT) érintő, **Follina** néven hivatkozott **kritikus nulladik napi** sérülékenység kapcsán, amelynek **aktív kihasználtsága** is ismert.

A sérülékenység a [CVE-2022-30190](https://cve.mitre.org/cve/2022/30190) számon került a nyilvántartásba. Sikeres kihasználás esetén a támadó egy **speciálisan szerkesztett MS Office dokumentum segítségével** az érintett rendszeren tetszőleges kódot futtathat, programokat telepíthet, adatokat tekinthet meg, módosíthatja vagy törölheti azokat, illetve új fiókokat hozhat létre az érintett felhasználó jogosultsági szintjének megfelelően.

Érintett verziók:

- Office 2013
- Office 2016
- Office 2019
- Office 2021
- valamint a Professional Plus kiadások

A sérülékenységgel kapcsolatban **gyártói hibajavítás még nem érhető el**, azonban a Microsoft közzétett egy tájékoztatót, amely tartalmazza a sérülékenység kihasználásának megelőzésére szolgáló [lépéseket](#).

Az NBSZ NKI fokozott óvatosságot javasol az e-mailek csatolmányaként érkező MS dokumentumok kapcsán!

Hivatkozások:

- <https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability>
- <https://securityaffairs.co/wordpress/131800/hacking/multiple-microsoft-office-versions-zero-day.html>
- <https://thehackernews.com/2022/05/chinese-hackers-begin-exploiting-latest.html>
- <https://www.helpnetsecurity.com/2022/05/31/cve-2022-30190-follina/>
- <https://nki.gov.hu/it-biztonsag/hirek/veszelyes-ms-office-zero-day-serulekenyseget-fedeztek-fel/>

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

TLP: WHITE