TLP:WHITE
Szabadon terjeszthető!

Riasztás
Microsoft Exchange szervereket érintő sérülékenységről

(2021. november 10.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet **riasztást** ad ki **Microsoft Exchange** szervereket érintő **magas kockázati besorolású sérülékenység** (CVE-2021-42321) **kapcsán**, mivel azt a támadók aktívan kihasználják. Sikeres kihasználás esetén a megfelelő jogosultsággal rendelkező támadó távoli kódfuttatást vihet végbe az érintett szerveren.

Érintett verziók: MS Exchange Server 2016; MS Exchange Server 2019

A Microsoft tájékoztatása szerint a hibát a parancssori változók nem megfelelő validálása okozza. A sérülékenység a helyi Exchange kiszolgálókat érinti (ideértve az Exchange Hybrid módban használtakat is), az Exchange Online szolgáltatás ügyfeleinek nem kell további lépéseket tenniük.
A fenti CVE számú sérülékenységre irányuló kihasználási kísérletek ellenőrizhetőek az alábbi PowerShell lekérdezés segítségével:

*Get-EventLog -LogName Application -Source "MSExchange Common" -EntryType Error | Where-Object { $_.Message -like "*BinaryFormatter.Deserialize*" }*

A Microsoft javasolja a Exchange Server Health Checker script használatát, amely segít észlelni a gyakori konfigurációs problémákat.
A Microsoft szeptemberben elérhetővé tette a **Microsoft Exchange Emergency Mitigation** (EM) nevű új Exchange Server szolgáltatást, amely automatikus védelmet nyújt a sebezhető Exchange-kiszolgálóknak.

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

Hivatkozások:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321
- https://www.bleepingcomputer.com/news/microsoft/microsoft-urges-exchange-admins-to-patch-bug-exploited-in-the-wild/

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