


Upozornění na problematické aktualizace pro Windows Server

 portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-problematicke-aktualizace-pro-windows-server

V rámci březnového balíku bezpečnostních aktualizací byly zahrnuty opravy, které obsahují chybu a mohou způsobit zaseknutí a restart doménového řadiče. Jedná se o KB5035855 (Server 2016) a KB5035857 (Server 2022). Chybu způsobuje memory leak v rámci Local Security Authority Subsystem Service (LSASS) procesu.

Mitigace

Microsoft vydal opravy KB5037422 (Windows Server 2022) a KB5037423 (Windows Server 2016) a je doporučeno je aplikovat bez zbytečného odkladu, pokud již byly instalovány předchozí problematické patche. Další případnou možností je odstranění problematických patchů, ale vzhledem k existenci nových patchů by toto neměla být primární volba.

Pro aplikaci zmíněných OOB (out-of-band) oprav je třeba jejich stažení z Microsoft update katalogu <https://www.catalog.update.microsoft.com/Search.aspx?q=2024-03%20Cumulative%20Update> a jejich instalace na dotčených doménových řadičích. Aktualizace není dostupná ve Windows update a nebude tedy nainstalována automaticky.

Zdroje

- <https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-windows-server-issue-behind-domain-controller-crashes/>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-fix-for-windows-server-crashes/>
- <https://learn.microsoft.com/en-us/windows/release-health/status-windows-server-2022#3271msgdesc>
- <https://learn.microsoft.com/en-us/windows/release-health/resolved-issues-windows-10-1607#3271msgdesc>

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

25. 03. 2024

Obsah

Reakce

Zatím žádné reakce na článek