CrowdStrike BSOD | Portál NÚKIB

portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/crowdstrike-bsod

CrowdStrike BSOD

> Aktualizováno: Společnost CrowdStrike již vydala opravenou verzi. Pokud postižená stanice s tímto softwarem po restartu v pořádku nastartuje, CrowdStrike Falcon Agent by si měl automaticky stáhnout opravenou verzi postiženého souboru a tím problém s BSOD vyřešit.

Aktualizace EDR nástroje CrowdStrike Falcon Agent na operačním systému Windows způsobuje BSOD (Blue screen of death)

V případě tohoto problému je nutné smazat soubory `C-00000291*.sys` ze složky `C:\Windows\System32\drivers\CrowdStrike` v nouzovém režimu a následně provést restart postižené stanice.

Návod na spuštění systému Windows v nouzovém režimu naleznete na stránkách společnosti Microsoft: https://support.microsoft.com/cs-cz/windows/spuštění-počítače-v-nouzovém-režimu-ve-windows-92c27cff-db89-8644-1ce4-b3e5e56fe234

```
del "C:\Windows\System32\drivers\CrowdStrike\C-00000291*.sys"
```

Pokud provozujete postižené systémy v cloudovém prostředí, doporučujeme se řídit postupy jednotlivých cloudových poskytovatelů.

- AWS: https://health.aws.amazon.com/health/status
- Azure: https://azure.status.microsoft/en-gb/status/
- Google Cloud: https://status.cloud.google.com/incidents/DK3LfKowzJPpZq4Q9YqP

Postup opravy v případě virtualizovaného systému na Azure

1. Přihlaste se do Azure Console --> Přejít na virtuální počítače --> Vyberte virtuální počítač
2. Vlevo nahoře na konzole --> Klikněte na: "Připojit" --> Klikněte na --> Připojit --> Klikněte na "Další způsoby připojení" --> Klikněte na: "Sériová konzola"
3. Po načtení SAC zadejte „cmd“ a stiskněte enter.
    - zadejte `cmd`příkaz
    - vepište:`ch -si 1`
4. Stiskněte libovolnou klávesu (mezerník). Zadejte přihlašovací údaje správce
5. Zadejte následující:
    - `bcdedit /set {current} safeboot minimal`
    - `bcdedit /set {current} safeboot network`
6. Restartujte VM
7. Volitelné: Jak potvrdit stav spouštění? Spustit příkaz:

    ```
    wmic COMPUTERSYSTEM GET BootupState
    ```

Další informace

---

https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19