

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **33** ze dne **11.4.2023**

NÚKIB upozorňuje na zranitelnost týkající se aplikace Microsoft Outlook

Upozorňujeme na zranitelnost CVE-2023-23397 týkající se aplikace Microsoft Outlook, kterou lze zneužít doručením speciálně upravené e-mailové zprávy na Outlook klienta. Aby se tak stalo, není potřeba interakce od uživatele. Při úspěšném zneužití zranitelnosti útočník získá Net-NTLMv2 hash oběti, který lze využít k pohybu v síti napadené organizace. Podle společnosti Microsoft je tato zranitelnost již zneužívána.

Speciálně upravený e-mail obsahuje UNC path, který odkazuje na SMB server útočníka. Při doručení e-mailu dojde k pokusu o NTLM autentizaci na daný server.

K vyhodnocení dopadu zranitelnosti lze využít skript od společnosti Microsoft. Odkaz je dostupný v sekci Zdroje.

Zranitelnost se týká všech podporovaných verzí Microsoft Outlook pro Windows, které byly vydány před datem 14. března 2023. Aktualizace, která zabraňuje zneužití této zranitelnosti, již byla vydána. Doporučujeme její bezodkladnou instalaci. Pokud instalace aktualizace nelze bezodkladně aplikovat, lze zneužití zranitelnosti omezit následovně:

1. Přidání uživatelů do Protected Users Security Group, která zabrání autentizaci za pomoci NTLM. Dané opatření ale může mít dopad na autentizaci i do jiných služeb v rámci organizace. Z tohoto důvodu se doporučuje aplikovat pouze na velmi kritické účty z pohledu bezpečnosti, jako jsou například doménové účty. Pro více informací ohledně tohoto doporučení sledujte dokumentaci od společnosti Microsoft odkazovanou níže.
2. Blokovat odchozí komunikaci z organizace na port TCP/445.

Zdroje:

- Dokumentace a skript pro audit dopadu zranitelnosti (<https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/>)
- Článek od Microsoft ke zranitelnosti CVE-2023-23397 (<https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/>)
- Dokumentace od Microsoft ke zranitelnosti CVE-2023-23397 (CVE-2023-23397 - Security Update Guide - Microsoft - Microsoft Outlook Elevation of Privilege Vulnerability)