

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **48** ze dne **17.10.2023**

NÚKIB upozorňuje na kritické zranitelnosti v knihovnách webových prohlížečů

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) upozorňuje na kritické zranitelnosti, které byly objeveny v aplikacích internetových prohlížečů (Chrome, Firefox, Edge a dalších). Pouhým zobrazením upraveného obrázku nebo videa i bez další uživatelské interakce (tzv. zero-click) může dojít ke vzdálenému spuštění cizího kódu (RCE) a ovládnutí aplikace nebo celého systému útočníkem. Zranitelnosti objevené v knihovně libwebp (sloužící pro zpracování obrazového formátu WebP) a libvpx (sloužící pro zpracování videoformátu VP8) jsou již aktivně zneužívány a pro zranitelnost v knihovně libwebp byl i zveřejněn proof-of-concept (POC) jejího zneužití.

Zranitelnost v knihovně libwebp má označení CVE-2023-4863 (CVSS 8.8) a byla zveřejněna 12. září 2023, zranitelnost v knihovně libvpx má označení CVE-2023-5217 (CVSS zatím neurčeno) a byla zveřejněna 28. září 2023.

Tyto knihovny jsou součástí různých aplikací a systémů (např. webové prohlížeče nebo operační systémy) a z pozice správce nebo uživatele není snadné ověřit, zda je aplikace zranitelná či nikoliv. Nekompletní seznam zranitelných aplikací je uveden níže.

Doporučujeme provést co nejdříve aktualizace zranitelných aplikací a neodkládat automatické aktualizace. Lze také očekávat, že aktualizace aplikací budou jejich tvůrci vydávat v průběhu následujících dnů.

Zranitelné aplikace a systémy (pozn. jedná se o nekompletní výčet nejpoužívanějších aplikací a systémů, o kterých je známo, že byly touto zranitelností postíženy. Další položky mohou být postupně doplňovány.):

- Apple iOS, iPad OS a macOS - opraveno 8. září
- Google Chrome - opraveno ve verzi 117.0.5938.132 vydané v 27. září
- Mozilla Firefox - opraveno ve verzích 118.0.1 a 115.3.1 vydané 28. září
- Microsoft Edge – opravena byla pouze zranitelnost knihovny libwebp ve verzích 109.0.1518.140 a 117.0.2045.31 vydaných 15. září, v současné době není zřejmé, zda je tento prohlížeč postižen i zranitelností knihovny libvpx.
- Aplikace využívající platformu Electron (např. Visual Studio Code, Microsoft Teams, Signal Desktop, Discord apod.).
- Knihovny jsou součástí operačních systémů Linux (např. Debian, Ubuntu nebo RedHat) - typicky se jedná o systémové balíčky pojmenované přímo jako libvpx a libwebp.
- Kancelářský software LibreOffice - opravena zranitelnost knihovny libwebp ve verzích 7.5.7 a 7.6.2 vydaných 26. září

Zdroj: NÚKIB