ESET objevil zranitelnosti v produktech Mozilla a ve Windows, zneužívají je útočníci napojení na Rusko

27.11.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Bezpečnostní experti společnosti ESET objevili dosud neznámou zranitelnost CVE-2024-9680 v produktech organizace Mozilla, kterou v praxi pro své útoky využívá APT skupina RomCom napojená na Rusko. APT (Advanced Persistent Threat) je označení pro uskupení kybernetických útočníků, kteří se zaměřují na pokročilé přetrvávající hrozby a obvykle mají podporu států. Následující analýza pak odhalila další zranitelnost typu zero-day v operačním systému Windows. Jedná se o tzv. chybu eskalace oprávnění (privilege escalation bug), nyní označenou jako CVE-2024-49039. Kritická zranitelnost v případě produktů Mozilla, kterou ESET objevil 8. října 2024, má dle klasifikace zranitelností CVSS skóre 9,8 z 10. Ruskem podporovaná skupina RomCom útočila během letošního roku na Ukrajině, v Evropě i v USA. Podle dat společnosti ESET oběti, které od 10. října 2024 do 4. listopadu 2024 navštívily webové stránky obsahující škodlivý kód, pocházely převážně z Evropy, včetně České republiky, a Severní Ameriky.

Pokud je útok zneužívající objevené zranitelnosti úspěšný, dochází ke spuštění škodlivého kódu typu exploit. Oběť přitom musí „pouze“ navštívit webové stránky, které jsou k tomuto účelu speciálně vytvořené. Tento útok bez další interakce uživatele se nazývá zero-click. Následně dochází k instalaci backdooru (tzv. zádních vrátek) APT skupiny RomCom na počítač oběti. Díky zadním vrátkům mohou útočníci provádět příkazy a stahovat další moduly do počítače oběti.

„Celý útok se skládá z vytvořené falešné webové stránky, která přesměruje potenciální oběť na server, který hostuje exploit, a pokud je exploit úspěšný, spustí se další škodlivý kód, který stáhne a spustí zadní vrátka skupiny RomCom. I když nevíme, jakým způsobem skupina distribuuje odkaz na falešnou webovou stránku, pokud oběť na stránku přistupuje pomocí zranitelného, neaktualizovaného prohlížeče, je na jejím počítači bez jakékoli další interakce spuštěn škodlivý kód,“ říká Robert Šuman, vedoucí pražské výzkumné pobočky společnosti ESET. „Chtěli bychom poděkovat organizaci Mozilla za její velmi rychlou reakci, kdy vydala opravu zjištěné zranitelnosti během jednoho dne,“ dodává.

Zranitelnost CVE-2024-9680 objevili analytici společnosti ESET 8. října 2024. Jedná se o chybu typu „use-after-free“ (zranitelnost UAF) ve funkci Animation timeline prohlížeče Firefox. Organizace Mozilla opravila zranitelnost 9. října 2024. Následující analýza odhalila chybu eskalace oprávnění (privilege escalation bug) v operačním systému Windows. Jedná se o zranitelnost typu zero-day, která je nyní označena jako CVE-2024-49039. Umožňuje spouštění kódu mimo bezpečné prostředí sandboxu prohlížeče Firefox. Společnost Microsoft vydala opravu pro tuto druhou zranitelnost 12. listopadu 2024.

„APT skupina RomCom, která je známá také pod jmény Storm-0978, Tropical Scorpius nebo UNC2596, je uskupení kybernetických útočníků napojených na Rusko. Provádí jak příležitostné útočné kampaně proti vybraným obchodním cílům, tak specificky zaměřenou špionáž. Skupina přesunula svou pozornost na špionážní operace určené k získání zpravodajských informací a doplnila jimi tak své konvenčnější kyberzločinecké aktivity. V roce 2024 jsme objevili její operace proti vládním subjektům, obrannému a energetickému sektoru na Ukrajině, farmaceutickému a pojišťovacímu sektoru v USA, právnímu sektoru v Německu a vládním subjektům v Evropě. S

ohledem na to, že v případě těchto útočných kampaní stačí, aby oběť navštívila škodlivý web a neměla aktualizovaný prohlížeč, jsou tyto útoky globálním rizikem a týkat se mohou i České republiky," vysvětluje Šuman z ESETu.

Zranitelnost CVE-2024-9680 z 8. října umožňuje zranitelným verzím webového prohlížeče Firefox, poštovního klienta Thunderbird a prohlížeče Tor spouštět kód v omezeném kontextu prohlížeče. V kombinaci s dosud neznámou zranitelností CVE-2024-49039 v operačním systému Windows, která má dle CVSS skóre 8,8 z 10, lze spustit libovolný kód v kontextu práv přihlášeného uživatele. Spojení těchto dvou zranitelností typu zero-day umožnilo skupině RomCom použít exploit, škodlivý kód, který nevyžaduje žádnou interakci ze strany uživatelů. Úroveň objeveného útoku je podle bezpečnostních expertů velmi pokročilá a poukazuje na to, že útočníci usilují o získání či vyvinutí dalších, skrytých schopností, které mohou využít ve svých útocích. Pokusy o zneužití zranitelností, které byly úspěšné, navíc skupině RomCom umožnily nasazení škodlivého kódu typu backdoor (tzv. zadní vrátka) v evidentně rozsáhlé útočné kampani.

Toto je minimálně podruhé, co byla skupina RomCom přistižena při zneužívání významné zranitelnosti typu zero-day v praxi. V červnu 2023 zneužila zranitelnost CVE-2023-36884 prostřednictvím programu Microsoft Word.

Podrobné technické informace najdete na webu welivesecurity.com. Další, doplňující informace od APT skupinách napojených na Rusko, najdete například také v tematickém dílu podcastu TruePositive.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-objevil-zranitelnosti-v-produktech-mozilla-a-ve-windows-zneuzivaji-je-utocnici-napojeni-na-rusko