MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci marec riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK. Objavila sa nová vishingová (telefonická) kampaň, v ktorej sa automat alebo zahraničný podvodník v angličtine predstaví ako zamestnanec Úradu vlády SR a od obete požaduje osobné informácie.

Vládna jednotka CSIRT asistovala pri riešení prieniku na virtuálne servery organizácie v konštituencii CSIRT.SK a následnom získavaní a analýze forenzných stôp. Kompromitácia systémov nastala po zneužití viacerých zraniteľností prítomných kvôli zastaranosti systémov. Bola potvrdená exfiltrácia dát. Zistené indikátory kompromitácie a použité taktiky nasvedčujú, že by za útokom mohla stáť čínska APT skupina Ethereal Panda.

Pokusov o zneužitie rôznych zraniteľností tento mesiac jednotka zaznamenala viacero. Neznámi útočníci sa pokúsili zneužiť zraniteľnosť ProxyNotShell odoslaním škodlivej požiadavky na mailservery Microsoft Exchange orgánu verejnej správy. Ak by sa útočníkom podarilo zraniteľnosť zneužiť, získali by možnosť vzdialenej exekúcie kódu na týchto serveroch. Viaceré organizácie prijali tiež škodlivé e-maily a súbory úloh pre e-mailového klienta Microsoft Outlook. Jednalo sa o pokusy o zneužitie novo objavenej kritickej zraniteľnosti MS Outlook, CVE-2023-23397, ktorá umožňuje útočníkom prístup k e-mailom, a tiež Net-NTLMv2 haše, ktoré je možné zneužiť pre prihlásenie sa do ďalších systémov v infraštruktúre obete.

V marci CSIRT.SK monitoroval niekoľko útokov typu DDoS na webové stránky viacerých štátnych organizácií vrátane MV SR (www.minv.sk), MO SR (www.mosr.sk), MZVaEZ SR (www.mzv.sk, foreign.gov.sk), NR SR (www.nrsr.sk), Ústavný súd SR (www.ustavnysud.sk). Zasiahnuté boli aj weby bankového sektora (NBS, Exim banka a J&T banka) a ŽSR (www.zsr.sk). Útoky boli vedené proruskými skupinami NoName057(16), Anonymous Russia a Killnet. Dané organizácie sa podľa vyjadrení skupín na ich telegramových kanáloch stali terčom útokov kvôli rozhodnutiu Slovenska poskytnúť ukrajinskej armáde stíhačky MIG 29 a všeobecne kvôli aktivitám na podporu Ukrajiny voči ruskej agresii.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Platforma Achilles zároveň obsahuje monitoring nedostupnosti webových domén. V marci navyše rozposlala varovanie pred kritickou zraniteľnosťou CVE-2023-23397 zasahujúcou klientov Microsoft Outlook,

ktorá umožňuje útočníkom získať prístup k e-mailom a Net-NTLMv2 haše. Tiež informovala majiteľov nepodporovaných a zraniteľných MS Exchange serverov o postupne zavádzanom opatrení spoločnosti Microsoft, ktoré bude viesť k blokovaniu doručovania správ z takýchto serverov na účty v službe Exchange Online.

Mesačník zraniteľností marec 2023

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
   - Microsoft Internet Explorer
   - Microsoft Edge
   - Mozilla Firefox
   - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
   - Microsoft .NET Framework
   - Oracle Java
6. Iné tohto mesačné závažné zraniteľnosti
   - SAP
   - FortiOS, FortiProxy
   - WiFi 802.11b

https://www.csirt.gov.sk/posts/3353/