MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

December 2022

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci december riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady predaja prístupových údajov do kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií na online fórach. Nepoľavila ani phishingová kampaň zameraná na občanov Slovenskej republiky, v ktorej útočníci predstierajúci totožnosť Europolu a vysokopostavených členov Polície SR posielajú svojim obetiam falošné predvolania kvôli prechovávaniu detskej pornografie a podobným sexuálnym deliktom. Opäť preto pripomíname, že Slovenské úrady obdobné dokumenty nikdy neposielajú online, ale doručujú ich štandardne v papierovej forme.

CSIRT.SK v decembri riešil kybernetický bezpečnostný incident spočívajúci v útoku hrubou silou na mailserver konštituenta. Neboli potvrdené úspešné pokusy. Ako najefektívnejšie riešenie odporučila jednotka nasadenie dvojfaktorovej autentifikácie. Ďalším útokom, ktorý jednotka riešila, bol SQL injection na webovú doménu.

Iný druh podozrivých dopytov bol hlásený zvnútra ďalšej organizácie v konštituencii CSIRT.SK. Jednalo sa o prístupy na darkwebové domény. Vyšetrovanie CSIRT.SK ukázalo, že sa jednalo o testovanie systémov a prístup k nelegálnej online knižnici. Vážnejšia situácia nastala v inej organizácii, z ktorej nelegitímne dopyty odchádzali na škodlivé domény, pravdepodobne C&C server útočníkov. Do tretice boli detegované interné dopyty resp. skenovanie siete z kompromitovaného zariadenia, ktoré CSIRT.SK podrobil forenznej analýze.

Zahraničný partner nahlásil v decembri Vládnej jednotke CSIRT skenovanie zraniteľností RCE v IP priestore Slovenskej republiky. Jednotka informáciu zdieľala s NBÚ. Zároveň prijala informáciu o prieniku do webovej domény štátnej organizácie zneužitím zraniteľnosti, ktorú preverovala. Iné hlásenie zase súviselo s verejne dostupnými API kľúčmi k vyvíjanej aplikácii štátnej organizácie v repozitári na platforme GitHub.

Vládna jednotka CSIRT sa v decembri stretla aj s netypickým prípadom, v ktorom základná škola požiadala o asistenciu a konzultáciu pri atribúcii zodpovednosti za vulgárne komentáre odoslané cez účty niekoľkých žiakov na platforme EduPage.

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. Jednotka rozšírila svoj monitoring o nedostupné webové domény. Tento mesiac detegovala nedostupnosť štátneho webu, ktorá bola následkom DDoS útoku proruskej skupiny NoName057(16).

Mesačník zraniteľností december 2022

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
    - Ubuntu Linux
    - FortiOS, FortiProxy
    - Foxit PDF Reader, Foxit PDF Editor

https://www.csirt.gov.sk/posts/3153.html?csrt=5448753193609764432