MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Január 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 január 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. Pokračovala niekoľkomesačná 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 ak Slovenské úrady obdobné dokumenty posielajú online, posielajú ich do elektronických schránok slovensko.sk alebo osobám, ktoré schránku nemajú aktivovanú, ich doručujú v papierovej forme.

CSIRT.SK prijal v januári informáciu o útoku typu DDoS na viaceré webové stránky spravované v Govnete (gov.sk), stránky televíznych staníc a bánk. K útoku sa prihlásila prorusky orientovaná hacktivistická skupina Anonymous Russia v súvislosti s podporou Slovenska Ukrajine voči súčasnej ruskej agresii.

Jednotka prijala hlásenie ransomvérového útoku, ktorý zasiahol správu obce a znefunkčnil dva počítače. To viedlo ku znefunkčneniu niekoľkých IT systémov, ktoré obec využíva. Ďalej boli hlásené prístupy na podozrivé domény z infraštruktúr dvoch ďalších organizácií v konštituencii CSIRT.SK.

Vládna jednotka CSIRT prijala v januári hlásenie od partnera o zraniteľnej verzii webovej redakčnej platformy Drupal a neprítomnosti zabezpečovacieho protokolu TLS na webovom sídle jednej organizácie, ktorú obratom informovala. Tiež informovala o kritickej zraniteľnosti vo firewalloch Sophos viacero organizácií, ktoré tento produkt podľa otvorených zdrojov používajú.

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.

Mesačník zraniteľností január 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
    - JSON Web Token
    - Git
    - VMware vRealize Log

https://www.csirt.gov.sk/posts/3303.html?csrt=13294354286461264077