MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

December 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

Mesiac december sa vzhľadom na množstvo a závažnosť kybernetických bezpečnostných incidentov v organizáciách štátnej a verejnej správy nahlásených Vládnej jednotke CSIRT niesol v pokojnejšom duchu.

Tradične v rámci svojej bežnej činnosti CSIRT.SK v mesiaci december 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.

Medzi zaujímavejšie riešené incidenty v decembri patrilo hlásenie NBÚ, ktorý poskytol VJ CSIRT indikátory kompromitácie masívnej spear-phishingovej kampane vedenej APT 28 (skupina je súčasťou ruskej vojenskej rozviedky GRU), ktorá zasiahla aj Slovensko. Cieľom kampane má byť doručenie malvéru Headlace, ktorý má viacero funkcií vrátane doručenia ďalších štádií infekcie/útoku, exfiltrovania citlivých údajov a vytvorenia zadných dvierok do infikovaného zariadenia. Doručenie škodlivého e-mailu v rámci danej kampane, slúžiaceho však iba na vylákanie prihlasovacích údajov obetí do e-mailových účtov, pozorovala jednotka CSIRT.SK u viacerých organizácií v Govnete. Slovenské ciele (kompromitované dôveryhodné e-mailové účty) mali hypoteticky slúžiť ako prostriedok pre ďalšiu fázu útoku. Nedá sa však vylúčiť, že sa v kybernetickom priestore SR šíria aj škodlivé e-maily obsahujúce spomínaný malvér. VJ CSIRT situáciu monitoruje a preveruje ďalšie možné potenciálne obete.

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. V súvislosti s minulomesačným incidentom cryptojackingu na cloudové prostredie organizácie vydala VJ CSIRT odporúčanie pre svoju konštituenciu na zabezpečenie prístupu cloudových služieb.

Mesačník zraniteľností december 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
    - Procesory AMD
    - SAP Business Technology Platform
    - Wordpress
    - ownCloud
    - Android
    - Produkty Atlassian
    - VMware

https://www.csirt.gov.sk/posts/3931.html?csrt=7331014190684610169