MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

November 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 november 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. Opakovane sme pozorovali spearphishingovú kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty. Nahlásené boli aj podvodné e-maily, v ktorých sa odosielatelia vydávali za predstaviteľov organizácií zodpovedných za kontrolu dodržiavania zákona. Obetiam posielali falošné súdne predvolania pod rôznymi zámienkami.

Vládna jednotka CSIRT riešila spear-phishingovú kampaň, ktorej útočníci zneužívali meno a e-mailovú adresu zamestnanca MIRRI SR. Kampaň sa zameriavala najmä na súkromné spoločnosti. Podvodné správy obsahovali prílohu so škodlivým VBS skriptom, ktorého analýzou jednotka zistila, že príloha mala za cieľ nainštalovať do kompromitovaného zariadenia trójsky kôň so zadnými dvierkami Remcos RAT. Tento umožňuje úplné prevzatie kontroly nad infikovaným zariadením. MIRRI SR vydalo varovanie, ktoré bolo publikované aj v ďalších médiách, napríklad: https://www.aktuality.sk/clanok/y5aeXn4/rezort-investicii-upozornil-na-kyberneticky-utok-ktory-zneuziva-nazov-ministerstva/

CSIRT.SK začal proces vyšetrovania kybernetického útoku na systém MetaIS (Centrálny metainformačný systém verejnej správy). Neznámy útočník sa pokúšal o zneužitie zraniteľnosti v systéme. Došlo ku „resetu“ servera Confluence s vymazaním databázy. Server skončil pri nabehnutí s chybou pre klientske časti, ktoré zlyhali. Útok sa teda útočníkovi nepodarilo vykonať až do bodu vytvorenia administrátorského účtu v systéme Confluence Server. Nepodarilo sa mu tak nad ním prebrať kontrolu.

VJ CSIRT prijala v novembri hlásenie kybernetického útoku typu cryptojacking na cloudové prostredie organizácie v jej konštituencii. Útočník získal administrátorský prístup do prostredia Microsoft Cloud a vytvoril niekoľko stoviek virtuálnych mašín. Tieto zneužil na ťažbu kryptomien, čím spôsobil škodu rádovo v desiatkach tisíc Eur. Zároveň vymazal tenant internej platformy MS Teams. Jednotka zaistila potrebné dáta a začala ich forenznú analýzu pre zistenie rozsahu incidentu.

Okrem toho jednotka CSIRT.SK riešila prípad exfiltrácie používateľských mien z webu organizácie v konštituencii CSIRT.SK. Webstránka je postavená na platforme Wordpress a útočník zneužil dostupný skript xmlrpc.php. Prevádzkovateľ webu zabránil pokračovaniu útoku tým, že daný skript, a teda

možnosť API volaní, zneprístupnil. Vzhľadom na častý výskyt podobných miskonfigurácií pripravuje CSIRT.SK návod ako bezpečne nakonfigurovať stránku postavenú na platforme Wordpress.

V novembri prijal CSIRT.SK hlásenie od občana, ktorý si všimol neplatný certifikát nasadený pre verejnú wifi v klientskom centre organizácie v konštituencii VJ CSIRT. Kedykoľvek Vás Vaše zariadenie upozorní, že wifi sieť, na ktorú sa pripájate, má neplatný certifikát, zbystrite pozornosť. Môže sa totiž jednať o útok typu man-in-the-middle, kde útočník predstiera totožnosť legitímnej wifi služby, zariadenia obetí sa pripájajú a komunikujú cez zariadenie útočníka a týmto spôsobom odchytáva a má pod kontrolou všetku komunikáciu.

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 slúži tiež na monitoring dostupnosti štátnych a verejných webových domén.

Mesačník zraniteľností november 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
    - Intel, AMD firmware
    - Zimbra Collaboration
    - SysAid
    - Microsoft Exchange
    - Exim
    - Linux glibc
    - Citrix NetScaler ADC, NetScaler Gateway
    - Atlassian Confluence Server

https://www.csirt.gov.sk/posts/3874.html?csrt=14322666289581170857