MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

November 2021

Vypracoval: CSIRT.SK

TLP: White

V mesiaci november sa stal jedným z najväčších bezpečnostných incidentov únik údajov spoločnosti GoDaddy. GoDaddy je jedným z najväčších svetových registrátorov domén a webhostingovou spoločnosťou, ktorá poskytuje svoje služby viac ako 20 miliónom zákazníkov po celom svete.

GoDaddy oznámila, že údaje až 1,2 milióna zákazníkov boli vystavené na milosť útočníkom po tom, čo získali prístup do firemného hostiteľského prostredia Managed WordPress. Incident bol objavený 17. novembra 2021, avšak útočníci mali prístup k systémom a údajom minimálne od 6. septembra 2021. Spoločnosť okamžite kontaktovala orgány činné v trestnom konaní, pričom médiám neposkytla podrobnosti o útoku, okrem toho, že útočník použil kompromitované heslo na prístup k dotačnému systému v jeho starých zdrojových kódoch pre Managed WordPress.

Managed WordPress je služba na vytváranie stránok, ktorá umožňuje spoločnostiam a jednotlivcom používať populárny systém správy obsahu WordPress (CMS) v hosťovanom prostredí bez toho, aby ho museli sami spravovať a aktualizovať.

Útočníci počas útoku získali prístup k údajom ako emailová adresa, zákaznícke číslo, pôvodné administrátorské heslá, používateľské mená a heslá pre sFTP a databázu a tiež súkromný SSL kľúč. Spoločnosť resetovala vystavené heslá a tiež vystavuje a inštaluje nové certifikáty.

Spoločnosť kontaktuje všetkých dotknutých zákazníkov, pričom zákazníci ju môžu priamo kontaktovať prostredníctvom centra pomoci, ktoré obsahuje konkrétne čísla podľa krajiny.

Od roku 2018 sa jedná už o piaty kybernetický incident spoločnosti GoDaddy. Obzvlášť bohatý na incidenty bol rok 2020. V marci roku 2020 útočník phishingovým útokom získal prístup k internému systému podpory a následne zmenil doménové mená záznamov niekoľkým zákazníkom. V máji toho istého roku spoločnosť uviedla, že útočníci ukradli prihlasovacie údaje k webhostingovým účtom zákazníkov (používateľské mená a heslá pre SSH). Posledným z útokov v roku 2020 bol tzv. „vishing“, ktorého pomocou útočníci získali kontrolu nad stránkami s kryptomenovými službami NiceHash a Liquid, kedy získali prístup k osobným informáciám o používateľoch.

Registrátor domén tvrdí, že tento únik mal vplyv aj na niekoľko jej značiek, ktoré predávajú služby Managed WordPress – 123Reg, Domain Factory, Heart Internet, Host Europe, Media Temple a tsoHost. Väčšinu týchto značiek získala spoločnosť GoDaddy v roku 2017 akvizíciou spoločnosti Host Europe Group.

Všetkým zákazníkom GoDaddy sa odporúča zapnúť si dvojfaktorovú autentifikáciu, skontrolovať si všetky súbory na svojom webe, najmä súbory v doplnkoch WordPress a adresároch tém, skontrolovať si všetky účty na svojej webovej stránke a odporúča sa taktiež byť obozretný pred ponukami ohľadom pomoci pri riešení tohto incidentu.

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. Jednotka riešila tiež prípady kompromitovaných e-mailových schránok zamestnancov inštitúcií vo svojej konštituencii, ktoré útočníci zneužili na rozposielanie phishingových e-mailov.

V zmysle zaujímavejších nahlásených kybernetických bezpečnostných incidentov dominovali novembru zraniteľnosti. CSIRT.SK preveroval a dohliadal na odstránenie zraniteľnosti typu SQL injection, možnosti tvorby podstránok na webovom sídle, implementáciu protokolu TLS na intranete a zamedzenie verejného prístupu na FTP server. Zraniteľnými systémami sa zaoberal aj v rámci svojej proaktívnej činnosti.

Jednotka sa zaoberala tiež medializovaným prípadom úniku cestovných dokladov delegácie Ministerstva hospodárstva SR na výstavu EXPO 2020 v Dubaji. Osobné doklady boli nájdené na portáli uloz.to. Vyšetrovanie ukázalo, že k úniku nedošlo dôsledkom kybernetického útoku.

CSIRT.SK informoval svoju konštituenciu o novej závažnej zraniteľnosti mailserverov Microsoft Exchange 2016 a 2019, CVE-2021-42321, ktorá môže útočníkom poskytnúť možnosť vzdialene vykonávať kód. Jednotka informovala aj o sofistikovanej phishingovej kampani majúcej za cieľ zneužitie tejto zraniteľnosti. Útočníci zneužívali predchádzajúcu legitímnu komunikáciu svojich obetí. Do vlákna pridali pozdrav a lákavú zámienku pre obeť, aby otvorila odkaz na škodlivú webstránku. Kampaň šírila malvér QakBot, DanaBot a SquirrelWaffle, ktorý umožňuje krádež citlivých informácií, či inštaláciu ransomvéru.

V rámci svojej proaktívnej činnosti jednotka vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Taktiež školí zamestnancov týchto organizácií. Témy preberané v novembri súviseli so základmi informačnej bezpečnosti a s bežnými hrozbami, s ktorými sa účastníci môžu stretnúť v pracovnom aj súkromnom živote. Účastníci získali informácie, ako tieto hrozby rozpoznávať a ako sa pred nimi brániť. Prezentácia ku školeniu je dostupná na našej webstránke.

Významné útoky vo svete

Platforma Robinhood sa stala obeťou úniku údajov o 7 miliónoch zákazníkov

Obchodná platforma Robinhood potvrdila únik údajov patriacich približne 7 miliónom zákazníkov. Na získanie prístupu k osobným údajom útočník použil sociálne inžinierstvo. Zavolal zamestnancovi zákazníckej podpory, ktorý mu (nevediac o tom, že sa jedná o útočníka) poskytol prístup k systémom. Únik zahŕňal emailové adresy 5 miliónov zákazníkov, celé mená 2 miliónov zákazníkov, meno, dátum narodenia a poštové smerovacie číslo pre 300 ľudí a ďalšie. Spoločnosť odporúča svojim zákazníkom byť obozretný pred phishingovými emailovými správami. Spoločnosť tiež uviedla, že si nie je vedomá toho, že by sa medzi uniknutými údajmi nachádzali čísla sociálneho poistenia, čísla bankových účtov alebo čísla debetných či kreditných kariet.

Kybernetický útok donútil spoločnosť Vestas Wind Systems uviesť svoje systémy do režimu offline

Spoločnosť Vestas Wind Systems uviedla svoje systémy vo viacerých obchodných jednotkách a lokalitách do režimu offline po tom, čo utrpela kybernetický útok. Niektoré továrne boli nútené spomaliť výrobu. Spoločnosť tiež potvrdila, že útočníkom sa podarilo získať informácie zo systémov, čo znamená, že niektoré údaje boli odcudzené. Vplyv na výrobu, konštrukciu a služby bol minimálny. Spoločnosť taktiež potvrdila, že pravdepodobne sa jedná o útok ransomvéru.

Spoločnosť Costco Wholesale v jednom zo svojich skladov našla zariadenie na skenovanie platobných kariet

Spoločnosť Costco Wholesale varovala svojich zákazníkov o potenciálnom odcudzení údajov o platobných kartách pri nakupovaní v jednom z jej obchodov. Spoločnosť nahlásila únik po tom, čo v jednom zo svojich skladov našla zariadenie na

skenovanie platobných kariet. Útočníci mohli ukradnúť meno, číslo karty, dátum vypršania platnosti karty a tiež kód CVV. Predajca odporučil zákazníkom, aby sledovali svoje bankové výpisy a výpisy z kreditných kariet kvôli podvodným poplatkom a nahlásili podozrivé transakcie príslušným finančným inštitúciám. Spoločnosť nezverejnila celkový počet dotknutých osôb, ani lokáciu skladu, kde sa zariadenie na skenovanie kariet našlo.

Incident, ktorý zasiahol zdravotné stredisko v Utahu, ohrozil údaje 582-tisíc pacientov

Zdravotné stredisko v Utahu zasiahol incident, ktorý ovplyvnil približne 582-tisíc pacientov. Incident sa stal 4. septembra 2021 a v ten istý deň bol aj vyriešený. Útočník, ktorý sa dostal do systémov, mohol mať prístup k údajom ako meno a priezvisko, emailová adresa, dátum narodenia, číslo sociálneho poistenia, číslo zdravotnej poisťovne a iné lekárske informácie. Centrum poukázalo, že si nie je vedomé toho, že by tieto údaje unikli online. To však nezaručuje, že žiadne ukradnuté údaje nie sú súkromne zdieľané medzi útočníkmi na darkwebe.

V Južnej Kórei vyčíňa spyware, ktorý sa zameriava na zariadenia s OS Android

Prebiehajúca kampaň s názvom PhoneSpy sa zameriava na juhokórejských používateľov pomocou aplikácií. V rámci kampane je na zariadenia s operačným systémom Android nasadený malvér, ktorý je schopný kradnúť citlivé údaje od používateľov a taktiež vie prevziať kontrolu nad mikrofónom a kamerou zariadenia. Spyware PhoneSpy sa pretvaruje napríklad za sprievodnú aplikáciu pre jógu, za aplikáciu Kakao Talk, prehliadač galérie obrázkov a ďalšie. Výskumníci zo spoločnosti Zimperium identifikovalo 23 aplikácií, ktoré sa javia ako neškodné. Okrem funkcií spyware-u sa niektoré aplikácie pokúšajú ukradnúť prihlasovacie údaje zobrazovaním rôznych falošných stránok.

Nový trójsky kôň CronRAT sa zameriava na internetové obchody

Výskumníci objavili nového trójskeho koňa (RAT) pre Linux, ktorý sa skrýva v úlohách naplánovaných na spustenie v neexistujúci deň – 31. februára. Malvér s názvom CronRAT sa zameriava na internetové obchody a umožňuje krádež údajov o kreditných kartách nasadením online skenerov platobných kariet na linuxové servery. Malvér zneužíva „cron“, čo je linuxový systém plánovania úloh. Útočníci, ktorí využívajú CronRAT by mohli na napadnutom serveri spustiť akýkoľvek kód. Nechvalnou výhodou je to, že tento malvér sa taktiež častokrát vyhýba detekcii.

Obchodný reťazec IKEA sa stal obeťou phishingových útokov

Útočníci sa zameriavajú na obchodný reťazec IKEA. Kradnú legitímne firemné emailové adresy a potom na nich odpovedajú odkazmi na škodlivé dokumenty, ktoré inštalujú malvér do zariadení príjemcov. Jedná sa o phishingové útoky, ktoré sa zameriavajú na interné poštové schránky spoločnosti IKEA. Tieto emailové správy rozposielajú aj iné napadnuté organizácie spoločnosti IKEA a jej obchodní partneri. IT tímy upozorňujú, že tieto emailové správy obsahujú odkazy so siedmimi číslicami na konci. Zamestnancom sa odporúča, aby emaily neotvárali a okamžite ich nahlásili IT oddeleniu.

Útočníci získali prístup k údajom na serveroch spoločnosti Panasonic

Spoločnosť Panasonic potvrdila únik údajov po napadnutí jej siete. K serverom v jej sieti nezákonne pristúpila tretia strana. Počas vyšetrovania sa zistilo, že útočníci získali prístup k niektorým údajom na súborovom serveri. Zatiaľ čo vydaná tlačová správa neobsahuje veľa podrobností týkajúcich sa času útoku, japonské predajne vrátane Mainichi a NHK uviedli, že útočníci mali prístup k serverom Panasonic medzi júnom

a novembrom. Útok na server spoločnosti Panasonic je súčasťou dlhej série incidentov týkajúcich sa japonských spoločností v posledných rokoch.

Ransomvér Yanluowang zasahuje americké organizácie minimálne od augusta roku 2021

Ransomvér Yanluowang sa zameriava na americké organizácie vo finančnom sektore pomocou malvéru BazarLoader. Na základe pozorovaných techník a taktík sa predpokladá, že útočníci môžu byť prepojení so skupinou Fivehands. Ransomvér zasahoval organizácie v USA minimálne od augusta roku 2021. Okrem finančného sektora útočili aj na výrobné spoločnosti, IT služby, poradenstvo a tiež strojárstvo. Po získaní prístupu k cieľovej sieti útočník používa PowerShell na stiahnutie nástrojov, ako je malvér BazarLoader, ktorý mu pomáha s laterálnym pohybom. Útočníci tiež hrozili útokmi DDoS a vymazaním údajov, ak obeť nesplní ich požiadavky.

Spoločnosť na testovanie DNA zasiahol únik údajov týkajúci sa viac ako 2 miliónov ľudí

Spoločnosť zaoberajúca sa analýzou DNA potvrdila únik údajov, ktorý sa týka približne 2,1 milióna ľudí. Uniknuté údaje zahŕňajú celé mená, čísla kreditných kariet a prislúchajúci CCV kód, čísla debetných kariet a prislúchajúci CVV kód, čísla účtov a heslá účtov do platformy. Kompromitovaná databáza obsahovala staršie údaje z rokov 2004 až 2012, pričom od roku 2012 nie je aktívna. Dotknutým osobám sa odporúča, aby boli ostražití voči podvodom a často sledovali výpisy svojich bankových účtov. Spoločnosť tvrdí, že neboli odhalené žiadne údaje z genetického testovania, pretože sú uložené v inom systéme.

Botnet EwDoor útočí na zariadenia s kritickou zraniteľnosťou CVE-2017-6079

Botnet EwDoor útočí na neopravené okrajové zariadenia EdgeMarc Enterprise Session Border Controller (ESBC) siete AT&T v amerických firmách. Botnet bol spozorovaný 27. októbra 2021, keď sa začali prvé útoky

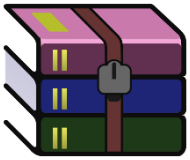
na zariadenia vystavené internetu, ktoré neboli opravené voči kritickej zraniteľnosti CVE-2017-6079. Za tri hodiny bolo zaznamenaných takmer 6-tisíc napadnutých zariadení. Výskumníci z 360 Netlab tvrdia, že botnet EwDoor sa pravdepodobne používa na DDoS útoky a ako zadné vrátka na získanie prístupu k sieťam cieľov. Tento botnet má 6 základných funkcií: aktualizácia, skenovanie portov, správa súborov, útok DDoS, reverzný shell a vykonávanie ľubovoľných príkazov na napadnutých serveroch.

- **Výskumníci objavili nový botnet Pink, ktorý infikoval viac ako 1,6 milióna zariadení.**
- **Akademickí výskumníci zverejnili informácie o novej metóde útoku, ktorú nazvali „Trojan Source“.**
- **Irán podozrieva Izrael a USA z útoku na iránske čerpacie stanice.**
- **Ransomvér HelloKitty pridáva ku svojim taktikám DDoS útoky.**
- **Kanadská provincia Newfoundland a Labrador utrpela kybernetický útok, ktorý viedol k narušeniu poskytovania zdravotnej starostlivosti.**
- **Ukradnutý SES token spoločnosti Kaspersky bol použitý v spear-phishingovej kampani.**
- **Cez 30-tisíc serverov GitLab stále nie je opravených voči kritickej zraniteľnosti, ktorá umožňuje vzdialené vykonanie kódu.**
- **Výskumníci spozorovali novú verziu bankového trójskeho koňa Mekotio.**
- **MediaMarkt bol zasiahnutý ransomvérom Hive.**
- **Skupina známa ako Lazarus sa zameriava na výskumníkov pirátskou verziou softvéru IDA Pro.**
- **Telnyx, poskytovateľ VOIP telefónie, sa stal obeťou DDoS útokov.**

- **Aplikácie „Smart TV remote“ a „Halloween Coloring“ na zariadeniach s operačným systémom Android obsahujú malvér.**
- **Skupina stojaca za ransomvérom Magniber zneužíva chyby v prehliadači Internet Explorer na infikovanie používateľov.**
- **Útočníci ostali neodhalení až 9 mesiacov na serveri dodávateľa vody v Queenslande.**
- **Nový botnet BotenaGo napísaný v programovacom jazyku Go sa zameriava na IoT zariadenia. Vo svojich útokoch využíva viac ako 30 rôznych exploitov.**
- **Inštalačný program operačného systému Windows 10 je zneužívaný na nasadenie malvéru BazarLoader.**
- **Aktivita bankového trójskeho koňa QBot je opäť na vzostupe.**
- **Falošná aplikácia s názvom SoSafe Chat distribuuje spyware na zariadenia s operačným systémom Android.**
- **Výskumníci objavili nový malvér SharkBot pre Android, ktorý kradne prihlasovacie údaje z bankových a kryptomenových služieb.**
- **Spoločnosť Microsoft varuje pred vývojom šiestich iránskych skupín.**
- **Štátom sponzorovaná severokórejská skupina sledovaná ako TA406 nasadzuje vlastný malvér na kradnutie informácií.**
- **Približne 6 miliónov smerovačov Sky Broadband obsahovalo kritickú zraniteľnosť, ktorej odstránenie trvalo takmer rok a pol.**
- **Iránsku leteckú spoločnosť Mahan Air zasiahol kybernetický útok, čo malo za následok uvedenie webovej stránky do režimu offline.**
- **Skupina útočníkov sa zameriava na biovýrobné zariadenia s novým vlastným malvérom Tardigrade.**
- **Útočníci zneužívajú chyby v platforme Microsoft MSHTML na špehovanie cieľových počítačov.**

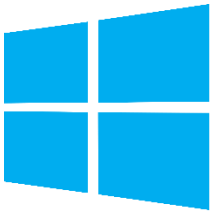
Závažné zraniteľnosti bežných softvérových produktov

Zraniteľnosť WinRAR umožňuje vykonávať kód



Výskumníci spoločnosti Positive Technologies odhalili zraniteľnosť obľúbeného archivátora WinRAR. Dovoľuje odchytávať a upravovať požiadavky, ktoré aplikácia posiela používateľovi. Po splnení istých podmienok ju môžu útočníci zneužiť na vzdialené vykonávanie kódu na zariadení obete. Spoločnosť WinRAR chybu opravila v júli tohto roka.

V serveroch Microsoft Exchange sa vyskytuje aktívne zneužívaná závažná zraniteľnosť



Spoločnosť Microsoft urguje používateľov, aby si aktualizovali svoje Exchange servery z dôvodu výskytu závažnej zraniteľnosti, ktorá je aktívne zneužívaná. Zneužitím môže dôjsť k vzdialenému vykonaniu ľubovoľného kódu autentifikovaným útočníkom v zraniteľnom systéme.

V module TIPC jadra Linuxu sa vyskytuje kritická zraniteľnosť umožňujúca vzdialené vykonanie kódu

Zraniteľnosť CVE-2021-43267 súvisí s pretečením medzipamäte haldy. Nachádza sa v module TIPC (Transparent Inter Process Communication) jadra Linuxu a jej zneužitím môže dôjsť k vzdialenému vykonaniu kódu. Dá sa zneužiť lokálne alebo vzdialene v rámci siete na získanie privilégií jadra a mohla by útočníkovi umožniť kompromitáciu celého systému.

Kritické zraniteľnosti Cisco

V produktoch Cisco boli opravené 4 kritické a viacero závažných zraniteľností.

TLP: White

CVE-2021-34795: Zraniteľnosť v službe Telnet v Cisco Catalyst PON Series Switches ONT by mohla umožniť neoverenému vzdialenému útočníkovi prihlásiť sa do postihnutého zariadenia pomocou debuggovacieho účtu.
CVE-2021-40112: Zraniteľnosť vo webovom rozhraní pre správu Cisco Catalyst PON Series Switches ONT by mohla umožniť neoverenému vzdialenému útočníkovi injektovať príkazy do postihnutého zariadenia.
CVE-2021-40113: Zraniteľnosť vo webovom rozhraní pre správu Cisco Catalyst PON Series Switches ONT by mohla umožniť neoverenému vzdialenému útočníkovi modifikovať konfiguračné súbory na zariadení.
CVE-2021-40119: Zraniteľnosť v mechanizme autentifikácie SSH založenom na kľúči v Cisco Policy Suite by mohla umožniť neoverenému vzdialenému útočníkovi prihlásiť sa do postihnutého systému ako používateľ root.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Intel® PROSet/Wireless WiFi and Killer™ WiFi Software, Intel® Processor, Intel® SSD DC Firmware, Intel® SoC Watch 2021, BIOS Reference Code a ďalšie. Úspešným zneužitím týchto zraniteľností môže dôjsť napríklad k eskalácii privilégií, úniku informácií alebo narušeniu dostupnosti služby.

Mesačník zraniteľností November 2021

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 závažné zraniteľnosti
    - Zraniteľnosť WinRAR umožňuje vykonávať kód
    - V serveroch Microsoft Exchange sa vyskytuje aktívne zneužívaná závažná zraniteľnosť

https://www.csirt.gov.sk/posts/2634.html?csrt=9018249930134539306