MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2021

Vypracoval: CSIRT.SK

TLP: White

Koncom januára a vo februári priniesli médiá informáciu o niekoľkých spoločnostiach, ktoré sa stali obeťou útoku na zariadenie File Transfer Appliance spoločnosti Accellion. Medzi zasiahnuté spoločnosti patria Kroger, Singtel, QIMR Berghofer Medical Research Institute, rezervná banka na Novom Zélande a ďalšie. Prvý zaznamenaný prípad z radu útokov v rámci tejto kampane bol práve útok na rezervnú banku na Novom Zélande, ktorý sme spomenuli v mesačnej správe z januára 2021.

Za útokmi pravdepodobne stoja skupiny prezývané UNC2546 a UNC2582. Skupiny sú spájané so skupinou stojacou za ransomvérom Clop a skupinou FIN11, avšak s tým rozdielom, že sa rozhodli nepoužiť malvér Clop na šifrovanie súborov. Zamerali sa na odcudzenie citlivých údajov.

Spoločnosť Accellion uvádza, že 20 rokov staré zariadenie FTA, kvôli ktorému došlo k útokom, používalo spočiatku približne 300 zákazníkov. Zasiahnutých bolo približne 100 zákazníkov, pričom menej ako 25 z nich utrpelo krádež dát významného rozsahu.

Podľa vyšetrovaní boli v útokoch zneužité štyri zero-day zraniteľnosti – CVE-2021-27101 až CVE-2021-27104. Spoločnosť tieto zraniteľné miesta v zariadení opravila, avšak zákazníkom dôrazne odporúča, aby prešli na aplikáciu Kiteworks. Tiež zverejnila dokument, v ktorom hlási koniec platnosti licencií ku 30. aprílu 2021.

Pri vyšetrovaní týchto incidentov bezpečnostní výskumníci zistili, že útočníci použili webový shell, ktorý nazvali DEWMODE. Útočník použil na získanie prístupu „SQL Injection“, potom nasledoval dopyt po ďalších prostriedkoch. Po získaní potrebnej úrovne prístupu útočník nasadil do systému webový shell DEWMODE.

Úlohou tohto shellu bola extrakcia zoznamu dostupných súborov z MySQL databázy. Útočníci ukradli údaje cez DEWMODE, ale nezašifrovali napadnuté systémy. Koncom januára obete začali dostávať vydieračské emaily, v ktorých sa útočníci vyhrážali zverejnením ukradnutých údajov. Pri analýze týchto emailov vyšetrovatelia zistili, že skupina FIN11 niektoré z IP adries a emailových účtov využívala pri phishingových kampaniach v období od augusta do decembra 2020.

Medzi zasiahnuté spoločnosti patrí aj kancelária štátneho audítora vo Washingtone. Organizácia odhalila kybernetický útok, pri ktorom mohlo dôjsť k odcudzeniu osobných údajov viac ako milióna ľudí.

Obeťou tejto série útokov je tiež spoločnosť Kroger. V rámci vyšetrovania útoku spoločnosť Kroger zistila, že narušením neboli dotknuté žiadne údaje o obchode s potravinami, vrátane platobných údajov. Unikli však údaje o ľudských zdrojoch a záznamy z lekárne a finančných služieb.

Medzi ďalšie zasiahnuté spoločnosti patria právnická firma Jones Day, Fugro, Danaher, Qualys, a NSW Transport. Všetky tieto spoločnosti utrpeli únik údajov spojený s útokom na platformu FTA od spoločnosti Accellion. Spoločnosti boli vydierané, že ukradnuté údaje budú zverejnené na webovej

stránke „CL0P^_- LEAKS" .onion. Motívom týchto útokov je pravdepodobne finančný zisk vzhľadom na to, že útočníci požadovali od obetí výkupné.

Riešené incidenty na Slovensku a z našej činnosti

Podobne ako v predchádzajúcich mesiacoch, CSIRT.SK aj v mesiaci február riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov.

Aj tento mesiac zachytila jednotka informácie o niekoľkých vishingových telefonátoch s tematikou technickej podpory Microsoftu. Podvodná kampaň však vykazovala prudko klesajúci trend.

CSIRT.SK prijal informáciu o opakovanom kurióznom útoku na online vyučovanie jednej základnej školy cez platformu Zoom. Jednalo sa o prvý incident tohto druhu, ktorý jednotka riešila. Bohužiaľ nešlo o jediný útok na školu, ktorý bol jednotke vo februári nahlásený. Iná škola utrpela útok ransomvérom, pri ktorom stratila mnohé cenné archivované dokumenty. Incident nahlásila niekoľko mesiacov po jeho odohratí.

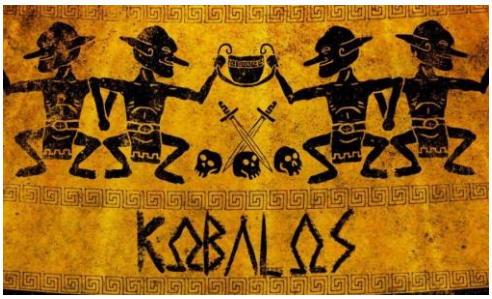
Vládna jednotka riešila niekoľko podozrení na únik citlivých informácií. V jednom prípade páchateľ ponúkal na predaj údajne odcudzenú databázu orgánu štátnej správy SR. S pomocou externého partnera sa jednotke podarilo získať spomínané dáta a v spolupráci s údajnou obeťou odhaliť, že išlo o falošné tvrdenie. Výsledky vyšetrovania boli potvrdené nezávislým vyšetrovaním incidentu národnou jednotkou SK-CERT pri NBÚ. CSIRT.SK tiež nahlasoval dotknutým subjektom únik prihlasovacích údajov do systémov FortiOS z databázy získanej od partnerskej európskej organizácie.

CSIRT.SK v rámci svojej proaktívnej činnosti vykonal testy niekoľkých webových portálov verejnej správy. Zaujímal sa aj o bezpečnosť mobilnej a webovej aplikácie Štatistického úradu pre sčítanie obyvateľov, domov a bytov 2021, v ktorej neodhalil závažné nedostatky. Ďalej informoval svoju konštituenciu o aktuálnych zdrojových IP adresách a iných indikátoroch kompromitácie nového variantu ransomvéru Ryuk.

Okrem vyššie uvedeného poskytla jednotka v niekoľkých prípadoch poradenstvo v technických a právnych záležitostiach.

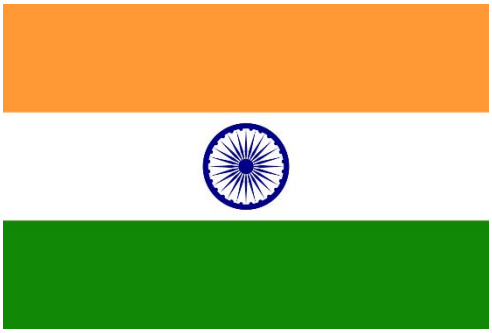
Významné útoky vo svete

Spoločnosť ESET objavila malvér Kobalos, ktorý kradne prihlasovacie údaje



Spoločnosť ESET objavila nový malvér Kobalos, ktorý sa zameriava na superpočítače po celom svete, pričom kradne prihlasovacie údaje pre bezpečné sieťové pripojenia pomocou infikovanej verzie softvéru OpenSSH. Kobalos je možné spustiť na unixových platformách, avšak môžu existovať aj varianty pre operačné systémy AIX a Windows. Kobalos poskytuje vzdialený prístup k súborovému systému a môže vytvárať terminálové relácie, čo umožňuje útočníkom spúšťať ľubovoľné príkazy. Súbor /usr/bin/sshfile bol nahradený upraveným spustiteľným súborom, ktorý zaznamenal používateľské meno, heslo a cieľový názov hostiteľa a zapísal ich do šifrovaného súboru.

V Indii došlo k úniku viac ako 8 miliónov výsledkov testov na COVID-19



V Západnom Bengálsku v Indii potenciálne uniklo viac ako 8 miliónov výsledkov testov na COVID-19. Etický hacker, ktorý objavil chybu na webovej stránke tvrdí, že unikli výsledky každého, kto absolvoval test na COVID-19. Chyba sa nachádzala v štruktúre URL odkazu, ktorý mal informovať ľudí o ich výsledkoch testov. Únik zahŕňa údaje o občanoch ako meno, vek, dátum a čas testovania vzorky, výsledok testu, adresu bydliska a podobne. Chyba na webovej stránke už bola opravená, avšak to nevylučuje, že k osobným údajom mohla pristúpiť tretia strana. Nie je však známe, že by k takémuto neoprávnenému prístupu naozaj došlo.

Bezpečnostné systémy spoločnosti StormShield boli napadnuté útočníkmi

STORMSHIELD

Francúzska spoločnosť StormShield zaoberajúca sa kybernetickou bezpečnosťou odhalila, že ich bezpečnostné systémy boli napadnuté útočníkmi. Získali prístup k tiketovaciemu systému a ukradli zdrojový kód pre softvér Stormshield Network Security firewall. Hlbšie vyšetrovanie naznačuje, že zdrojový kód

nebol zmenený. Únik tohto zdrojového kódu môže útočníkom uľahčiť hľadanie zraniteľností, ktoré môžu následne zneužiť. Incident môže mať rozsiahly dopad, keďže tento softvér používajú francúzska vláda, obranné agentúry a európsky trh SMB.

Vývojár hier CD Projekt Red utrpel útok ransomvérom

Poľský vývojár hier CD Projekt Red sa stal obeťou útoku ransomvérom. Útočník získal prístup do podnikovej siete spoločnosti. Zatiaľ čo niektoré zariadenia v sieti sú šifrované, zálohy ostali nedotknuté. Útočníci tvrdia, že získali kópie zdrojového kódu pre hry Cyberpunk 2077, Gwent a The Witcher 3, spolu s nevydanou verziou tejto hry. Výrobcovia hry uviedli, že výkupné nezaplatia, pretože to aj tak nakoniec môže viesť k zverejneniu ukradnutých údajov. Skupina útočníkov stojaca za týmto útokom bola identifikovaná pod názvom HelloKitty.

Útočníci pristúpili k verejne dostupnej databáze spoločnosti Emsisoft

Poskytovateľ antivírusových riešení Emsisoft potvrdil, že tretia strana mala prístup k verejne prístupnej databáze obsahujúcej technické logy. Podľa spoločnosti išlo o nesprávnu konfiguráciu, ktorá vyústila do vystavenia databázy testovacieho systému. Spoločnosť Emsisoft tvrdí, že okamžite uviedla systém do režimu offline a začala vyšetrovanie veci. Výsledkom bolo zistenie, že osobné informácie v databáze zahŕňali len 14 emailových adries 7 rôznych organizácií.

Spoločnosť AFTS bola zasiahnutá kybernetickým útokom

Útok ransomvérom na platobný procesor spoločnosti ATFS (Automatic Funds Transfer Services) spôsobil únik údajov mnohých miest a agentúr v Kalifornii a vo Washingtone. Kybernetický útok spôsobil značné narušenie obchodných operácií spoločnosti AFTS, čím zneprístupnil ich webové stránky a ovplyvnil spracovanie platieb. Za útokom stojí skupina útočníkov s názvom „Cuba ransomware“, ktorá ukradnuté údaje

začala predávať na svojich stránkach. Útočníci tvrdia, že ukradli finančné a daňové dokumenty, korešpondenciu so zamestnancami bánk, pohyby na účtoch a podobne. Potenciálne vystavené údaje sa líšia v závislosti od mesta alebo agentúry, ale môžu zahŕňať mená, adresy, telefónne čísla, ŠPZ, čísla VIN, informácie o kreditných kartách, šeky a fakturačné údaje.

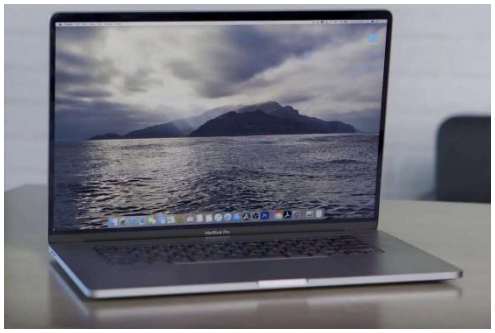
Spoločnosť Sequoia Capital utrpela únik údajov po neúspešnom BEC útoku

Americká firma Sequoia Capital zverejnila informáciu o úniku údajov po neúspešnom BEC útoku. Neoprávnená tretia strana získala vzdialený prístup k emailovej schránke jedného zo zamestnancov. Nezískali prístup k ďalším zdrojom a aktívam v sieti spoločnosti. Aj keď incidentom bola zasiahnutá len jedna poštová schránka, spoločnosť nevylučuje, že mohlo dôjsť k exfiltrácii osobných údajov. Sequoia uviedla, že nenašla nijaké dôkazy o tom, že by exfiltrované údaje boli predávané alebo bolo nimi akokoľvek manipulované. Spoločnosť o útoku informovala aj príslušné orgány činné v trestnom konaní a do budúcna prijala sériu opatrení pre podobné incidenty.

LodaRAT sa okrem operačného systému Windows zameriava aj na Android

LodaRAT, ktorý zasahoval zariadenia s operačným systémom Windows sa zameriava aj na zariadenia s Androidom. Taktiež bola identifikovaná aj aktualizovaná verzia pre Windows, pričom obe verzie boli zachytené pri nedávnej kampani na Bangladéš. Zatiaľ čo predchádzajúce verzie malvéru LodaRAT sa zväčša používali na kradnutie poverení, novšie verzie prichádzajú so súborom príkazov na zhromažďovanie informácií. LodaRAT je trójsky kôň, ktorý prichádza s rôznymi schopnosťami špehovania obetí, ako napríklad zaznamenávanie vstupov mikrofónov a webových kamier na zariadeniach obetí. Názov „Loda“ je odvodený od adresára, do ktorého sa autor škodlivého softvéru rozhodol zapísať záznamy keyloggerov.

Malvér Silver Sparrow infikoval takmer 30-tisíc zariadení Mac



Nový malvér pre macOS známy ako Silver Sparrow potichu infikoval takmer 30-tisíc zariadení Mac v 153 krajinách sveta. Účel tohto malvéru je neznámy. Objavili ho bezpečnostní výskumníci zo spoločností Red Canary, Malwarebytes a VMware Carbon Black, pričom sa vyznačuje neobvyklými vlastnosťami, vrátane komponentu zostaveného pre nový čip Apple M1. Bola spozorovaná distribúcia tohto malvéru formou dvoch rôznych súborov s názvom „updater.pkg“ alebo „update.pkg“. Jediný rozdiel medzi nimi je ten, že update.pkg obsahuje binárne súbory pre procesory Intel x86_64 aj Apple M1, zatiaľ čo updater.pkg obsahuje iba spustiteľný súbor pre Intel.

V meste Oldsmar na Floride došlo k útoku na systém na úpravu vody

Neznámy útočník získal prístup k systému na úpravu vody v meste Oldsmar na Floride. Pokúsil sa zvýšiť koncentráciu hydroxidu sodného na mimoriadne nebezpečnú úroveň. K útoku došlo prostredníctvom softvéru TeamViewer, ktorý slúži na vzdialené riešenie problémov so systémom. Prevádzkovateľ uviedol, že spozorovali, ako niekto prevzal kontrolu nad myšou a pomocou nej vykonával zmeny v softvéri, ktorý slúži na ovládanie úprav vody v meste. Útočník strávil vo vnútri systému tri až päť minút a zmenil hladinu hydroxidu sodného zo 100 ppm (častíc NaOH na milión častíc) na 11 100 ppm. Keďže operátor okamžite zasiahol, obyvatelia mesta Oldsmar neboli ohrození.

Holandská organizácia pre výskum (NWO) utrpela útok na servery

Servery patriace Holandskej organizácii pre výskum (NWO) boli kompromitované, čo prinútilo organizáciu, aby znefunkčnila svoju sieť a pozastavila prideľovanie grantov. Úlohou NWO je investovať do výskumu a výskumnej infraštruktúry s cieľom zvýšiť kvalitu a inovácie vo vede. NWO tvrdí, že útok nemal vplyv na jej webové stránky. Zdá sa, že nebol infikovaný ani externý server hostiaci aplikáciu ISAAC a systém podávania

žiadostí o granty, ktorý používajú žiadatelia na predloženie návrhov. Server ISAAC bol vypnutý, až kým nebude vyvrátené podozrenie na infekciu malvérom. Výsledkom je, že procesy SIA a NRO zostávajú pozastavené na neurčito. Organizácia tiež informuje, že neposkytne ďalšie podrobnosti o útoku a o tom, ako k nemu došlo, zatiaľ čo prebieha vyšetrovanie a obnova systému.

V spoločnosti Yandex došlo k neoprávnenému prístupu k tisícom poštových schránok používateľov

Ruská spoločnosť Yandex prevádzkujúca emailovú službu a internetový vyhľadávač dnes oznámila, že jeden z jej správcov systému povolil neoprávnený prístup k tisícom poštových schránok používateľov. Vyšetrovanie odhalilo, že konanie zamestnanca viedlo ku kompromitácii takmer 5-tisíc emailových schránok Yandex. Zamestnanec bol správcom systému, ktorý mal prístupové práva na poskytovanie technickej podpory pre emailovú službu spoločnosti Yandex. V tlačovej správe spoločnosť uviedla, že správca to urobil „pre osobný prospech“. Bezpečnostný tím spoločnosti Yandex zablokoval neoprávnený prístup k napadnutým poštovým schránkam.

- Malvér Agent Tesla používa nové techniky na obchádzanie obranných bariér.
- Trickbot mapuje siete obetí pomocou nástroja „masscan“.
- Malvér Hildegard je súčasťou jedného z najkomplikovanejších útokov zameraných na Kubernetes.
- Nový dekóder pre ransomvér Fonix dokáže zadarmo obnoviť súbory obetí.
- Nový botnet Matryosh sa zameriava na zariadenia so systémom Android.
- Spotify utrpel druhý kybernetický útok za posledné 3 mesiace.
- Spoločnosti Eletrobras a Copel boli zasiahnuté ransomvérom.
- Spoločnosť WestRock sa stala obeťou útoku ransomvérom.
- Škodlivé rozšírenie v prehliadači Chrome zneužíva synchronizáciu na odcudzenie údajov používateľov.
- Nový phishingový útok používa morzeovku na skrytie škodlivých odkazov.
- Ransomvér Ziggy sa vypne a uvoľní dešifrovacie kľúče.
- Aplikácia na skenovanie čiarových kódov v obchode Google Play sa po aktualizácii transformuje na malvér.
- Poskytovateľ prostriedkov na vývoj webu SitePoint, upozornil používateľov na únik údajov.
- Nový malvér BendyBear je prepojený s čínskou hackerskou skupinou.
- CISA tvrdí, že veľa obetí útokov na SolarWinds nemalo priame spojenie so SolarWinds.
- Organizácia pre výskum a inovácie vo Veľkej Británii čelila útoku ransomvérom.
- Vojenské a jadrové subjekty sú cieľom nového malvéru pre Android.
- Spoločnosť Microsoft varuje pred zvyšujúcim sa počtom útokov s použitím webových shellov.

- **DDoS útoky vyradili výmenné servery kryptomeny EXMO.**
- **Severokórejskí hackeri sa pokúsili preniknúť do počítačových systémov spoločnosti Pfizer.**
- **Nesprávne nakonfigurované detské monitory umožňujú neoprávnené sledovanie.**
- **Spoločnosť Kia Motors America sa stala obeťou útoku ransomvérom. Útočníci požadujú 20 miliónov dolárov.**
- **Trójsky kôň Masslogger kradne osobné údaje z Outlooku a prehliadača Chrome.**
- **Útočníci stojaci za útokom na SolarWinds stiahli časť zdrojového kódu Azure a Exchange.**
- **RIPE NCC odhalil neúspešný útok hrubou silou na svoju SSO službu.**
- **Nová skupina LazyScripter sa zameriava na letecké spoločnosti.**
- **Ransomvér Ryuk sa sám rozširuje vo Windows zariadeniach v lokálnej sieti.**
- **Skupina s názvom Hotarus Corp kompromitovala ministerstvo financií v Ekvádore a najväčšiu banku v krajine.**

Závažné zraniteľnosti bežných softvérových produktov

Závažná zraniteľnosť v knižnici GnuPG Libgcrypt

V knižnici GnuPG Libcrypt existuje vysoko závažná zraniteľnosť v spôsobe dešifrovania dát. Útočníkom umožňuje spôsobiť zrútenie aplikácie, ktorá knižnicu používa, alebo vzdialene vykonávať kód. Toto je možné dosiahnuť jednoducho dešifrovaním špeciálne upraveného balíka dát.

Baron Samedit: eskalácia privilégií v linuxovom nástroji Sudo

V programe Sudo, ktorý umožňuje vykonávať vybrané operácie s právami používateľa root v operačných systémoch Unix/Linux, bola opravená kritická zraniteľnosť. Nazvaná ako „Baron Samedit“ bola objavená bezpečnostnou auditnou spoločnosťou Qualys a umožňuje získať oprávnenia používateľa root každému lokálnemu používateľovi. Zraniteľnosť sa v programe Sudo nachádzala 9 rokov.

Spoločnosť Apple opravila závažné bezpečnostné zraniteľnosti v operačnom systéme iOS a iPadOS. Tri sú aktívne zneužívané.

Spoločnosť Apple vydala aktualizáciu, ktorá opravila aj 3 závažné zero-day zraniteľnosti, ktoré by mohli byť zneužité na kompromitáciu zariadenia vzdialeným útočníkom a vzdialené vykonávanie kódu. Zraniteľnosti sa nachádzajú v jadre operačného systému a v platforme webového prehľadávania WebKit.

V komponente V8 prehliadača Chrome bola opravená aktívne zneužívaná zero-day zraniteľnosť

V prehliadači Chrome spoločnosti Google bola opravená aktívne zneužívaná zraniteľnosť, ktorá existuje v komponente V8. Jedná sa o pretečenie medzipamäte haldy. Spoločnosť Google zatiaľ nezverejnila viac informácií. Chce počkať, kým si väčšina používateľov nainštaluje najnovšiu dostupnú aktualizáciu.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero závažných zraniteľností a žiadna kritická:
Zraniteľnosti *CVE-2020-12374, CVE-2020-12377, CVE-2020-0544, CVE-2020-0521, CVE-2020-12362, CVE-2020-24450* a *CVE-2020-8701* môžu autentifikovanému používateľovi umožniť eskaláciu privilégií cez lokálny prístup.
Zraniteľnosti *CVE-2020-12361* a *CVE-2020-24482* môžu neautentifikovanému používateľovi umožniť narušiť dostupnosť systému cez sieťový prístup.

Kritické zraniteľnosti Cisco

Spoločnosť Cisco opravila viacero závažných a 9 kritických zraniteľností:
CVE-2021-1393: Zraniteľnosť v Cisco Application Services Engine môže neautentifikovanému vzdialenému útočníkovi umožniť získať prístup k privilegovanej službe na zraniteľnom zariadení.
CVE-2021-1289 až CVE-2021-1295: Zraniteľnosti vo webovom rozhraní pre správu VPN smerovačov RV160, RV160W, RV260, RV260P a RV260W môžu vzdialenému neautentifikovanému útočníkovi umožniť vykonávať ľubovoľný kód ako užívateľ root na zraniteľnom zariadení.
CVE-2021-1299: Zraniteľnosť vo webovom rozhraní na správu pre produkty SD-WAN môže autentifikovanému vzdialenému útočníkovi umožniť injektovať príkazy, vďaka čomu by mohol získať rootovské oprávnenia.

Mesačník zraniteľností Február 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 Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Závažná zraniteľnosť v knižnici GnuPG Libgcrypt
    - Spoločnosť Cisco vydala bezpečnostné aktualizácie pre svoje produkty
    - Baron Samedit: eskalácia privilégií v linuxovom nástroji Sudo
    - Spoločnosť Apple opravila závažné bezpečnostné zraniteľnosti v operačnom systéme iOS a iPadOS. Tri sú aktívne zneužívané.
    - Spoločnosť Cisco opravila 9 zraniteľností vo webovom rozhraní pre správu VPN smerovačov
    - V komponente V8 prehliadača Chrome bola opravená aktívne zneužívaná zero-day zraniteľnosť

https://www.csirt.gov.sk/aktualne-7d7.html?id=238