MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Január 2021

Vypracoval: CSIRT.SK

TLP: White

Phishingové kampane sú vo svete na dennom poriadku. Útočníci sú vďaka tejto technike schopní získať rôzne údaje od svojich obetí a následne ich využiť vo svoj prospech.

Spoločnosť Google vydala rady, ako odlíšiť „priateľa od nepriateľa“. Google a vedci zo Standfordu študovali phishingové kampane po dobu piatich mesiacov, pričom dospeli k záveru, že cieľom sú najčastejšie USA a Spojené Kráľovstvo. Vo svojom výskume zistili, že kampane priemerne trvali 1 až 3 dni a útočníci sa zamerali na 100 až 1000 obetí.

Dve nové phishingové taktiky na neoprávnené získavanie údajov využívajú automatizované odpovede platformy na obchádzanie e-mailových filtrov. Pri prvom spôsobe sa útočníci zameriavajú na presmerovanie legitímnych „out-of-office“ odpovedí zamestnancov. Pri druhom manipulujú s potvrdeniami o prečítaní. Tieto taktiky ukazujú, že útočníci využívajú všetky dostupné nástroje a medzery vo svoj prospech v nádeji o úspešný pokus o kompromitáciu účtu.

V poslednej dobe bola objavená súprava nástrojov s názvom LogoKit určená na prípravu phishingových kampaní. Táto súprava automaticky sťahuje logá spoločností. Útočníci tak môžu jednoducho napodobňovať rozličné prihlasovacie stránky, vrátane služieb SharePoint, OneDrive a Office 365.

LogoKit v reálnom čase mení logá a text na phishingovej stránke tak, aby sa prispôsobila cieľovým obetiam. Spoločnosť RiskIQ uviedla, že za mesiac identifikovala inštalácie LogoKit na viac ako 700 doménach. Po vstúpení na stránku sa email obete automaticky vyplní do poľa emailu alebo používateľského mena, čo obeti navodí pocit, že sa už na stránku predtým prihlásila.

Útoky s použitím nástroja LogoKit sú len podmnožinou všetkých phishingových útokov páchaných vo svete. Napríklad od mája roku 2020 prebieha phishingová kampaň, ktorá sa zameriava na vysoko postavených riadiacich pracovníkov spoločností vo výrobnom, realitnom, finančnom, vládnom a technologickom sektore s cieľom získať citlivé údaje.

Zraniteľnosť vyskytujúca sa v aplikácii TikTok mohla útočníkovi umožniť vybudovať databázu osobných údajov používateľov a ich telefónnych čísel. Zraniteľnosť, ktorá bola nahlásená a opravená ešte pred jej zverejnením, existovala vo funkcii „Nájsť priateľov“ mobilnej aplikácie TikTok. Táto funkcia umožňuje používateľom nájsť svojich priateľov buď prostredníctvom svojich kontaktov, Facebooku alebo pozvaním priateľov. Útočník s takým stupňom citlivých informácií by mohol vykonávať celý rad škodlivých aktivít, ako je napríklad phishing alebo iná trestná činnosť.

Prevádzkovatelia phishingovej kampane zameranej na stavebníctvo a energetiku odhalili údaje odcudzené pri útokoch, ktoré boli verejne viditeľné pomocou jednoduchého vyhľadávania na stránkach spoločnosti Google. Útok začal jednou z niekoľkých podvodných e-mailových šablón, pričom predmet emailu obsahoval meno zamestnanca cieľovej spoločnosti. Útočníci do emailu zahrnuli priložený HTML súbor obsahujúci vložený kód JavaScript, ktorého účelom bolo kontrolovať používanie hesiel.

Po svete sa šíria aj podvodné správy o limitácii účtu na službe PayPal. Kliknutím na odkaz v správe sa obeť dostane na podvodnú stránku, kde má zadať prihlasovacie údaje. Po falošnom prihlásení sú citlivé údaje odosielané útočníkom.

Phishing je vo všeobecnosti stará, ale stále veľmi obľúbená technika na zisk citlivých údajov. Aj napriek tomu, že existujú nástroje, ktoré tento typ útoku detegujú, útočníci ho stále využívajú a vylepšujú spôsoby jeho realizácie.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci január riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Vyskytli sa ešte ojedinelé prípady minulo-mesačnej kampane, kedy útočníci rozposielali phishing zo schránok zamestnancov štátnych organizácií. Prístup k ich účtom získali v dôsledku úspešného phishingového útoku, pri ktorom útočníci sa dostali ku prihlasovacím údajom svojich obetí.

Jednotka riešila medializovaný prípad, kedy sa neznámy páchateľ vydával za pracovníka Ministerstva práce, sociálnych vecí a rodiny SR a adresy na službe Gmail odosielal pod jeho hlavičkou falošné správy. V januári bol riešený tiež podobný prípad, kde spoločnosť IDS Slovakia nekalým spôsobom ponúkala prenájom .com domén. O tejto veci sme informovali aj na našej webstránke.

Jednotka naďalej sledovala priebeh podvodnej telefonickej kampane, v ktorej sa zahraniční podvodníci vydávajú za technickú podporu Microsoftu, alebo inej všeobecne známej technologickej firmy a obetiam tvrdia, že ich zariadenia majú zraniteľnosť, alebo boli napadnuté hackermi.

CSIRT.SK v rámci svojej proaktívnej činnosti vykonal opakovaný test IT systémov zdravotníckych zariadení SR dostupných z internetu s cieľom zistiť stav odstraňovania nahlásených zraniteľností v predchádzajúcich mesiacoch. Svoju konštituenciu informoval o niekoľkých únikoch údajov, resp. podozreniach na únik, a tiež o miskonfiguráciách niekoľkých webstránok.

Okrem toho nahlásil CSIRT.SK 22.1. NCZI medializovanú zraniteľnosť v systéme Moje eZdravie. Následne deň na to a dva dni na to prijal hlásenie o tejto zraniteľnosti od dvoch nahlasovateľov. V tom čase bola však už opravená. Nápravu vykonalo NCZI ešte večer 22.1., asi štvrť hodiny po nahlásení Vládnou jednotkou CSIRT. Na základe tohto incidentu vykonala jednotka testovanie na zraniteľnosti niekoľkých aplikácií NCZI. Nálezy boli odovzdané NCZI pre ich odstránenie.

Významné útoky vo svete

Spoločnosť T-Mobile utrpela únik údajov, ktorý zasiahol približne 200 tisíc zákazníkov

Americký poskytovateľ telekomunikácií T-Mobile utrpel únik dát. Kybernetický tím spoločnosti odhalil a zastavil neoprávnený prístup k informáciám. Uniknuté údaje zahŕňali napríklad telefónne čísla a v niektorých prípadoch aj informácie týkajúce sa hovorov. Nezahŕňali mená, fyzické ani emailové adresy, finančné údaje a podobne. Spoločnosť T-Mobile uviedla, že únik mal dopad na približne 200 tisíc zákazníkov. Jedná sa o štvrté narušenie bezpečnosti za posledné 3 roky.

Na fóre boli zverejnené údaje o 10 tisíc používateľoch kreditnej karty American Express

Útočník na fóre zdarma zverejnil údaje o 10-tisíc držiteľoch kreditných kariet American Express v Mexiku. V príspevku tvrdí, že získal údaje aj o zákazníkoch spoločnosti Santander a Banamex. Uniknuté údaje zahŕňajú celé čísla účtov a osobné identifikačné údaje zákazníkov (PII) vrátane mena, adresy, telefónneho čísla, dátumu narodenia, pohlavia a podobne. Útočník sa vyjadril, že neplánuje tieto údaje využívať na finančné podvody, ale na marketing alebo spam. Spoločnosť American Express nepoprela, ale ani nepriznala, že došlo k narušeniu ochrany údajov, ale zdieľala, že žiaden držiteľ karty nie je vystavený podvodným poplatkom.

Taliansky operátor Ho Mobile utrpel únik údajov. Dotknutých je približne 2,5 milióna používateľov

Taliansky operátor Ho Mobile uviedol, že došlo k ukradnutiu časti databázy zákazníkov. Útočníci získali osobné údaje o zákazníkoch a technické údaje SIM kariet. Táto databáza je na predaj na dark webe už od 22. decembra 2020. Obsahuje dostatočné podrobnosti na uskutočnenie útokov typu SIM-swap. Útok sa týka približne 2,5 milióna zákazníkov. Uniknuté údaje o používateľoch konkrétne zahŕňajú meno, priezvisko,

telefónne číslo, email, dátum a miesto narodenia, národnosť a adresu zákazníka. Útočníci tiež získali údaje ako identifikačné číslo integrovanej SIM karty. Spoločnosť ponúka bezplatnú výmenu SIM kariet.

Útok na službu zdieľania súborov mohol spôsobiť odhalenie komerčných a citlivých údajov zákazníkov banky na Novom Zélande

Rezervná banka Nového Zélandu, známa ako Te Pūtea Matua, utrpela únik údajov po tom, čo útočníci hackli službu zdieľania súborov FTA (File Transfer Application) od spoločnosti Accellion. Táto banka je zodpovedná za tvorbu menovej politiky na stabilizáciu cien v krajine. Útočníci neoprávnene získali prístup k údajom uloženým u poskytovateľa služieb tretích strán. Narušenie bezpečnosti bolo obmedzené, avšak mohlo odhaliť komerčné a osobné citlivé údaje. Zdá sa, že hlavnou príčinou incidentu je kritická zraniteľnosť v FTA, ktorú spoločnosť Accellion identifikovala v polovici decembra, a ktorá bola okamžite riešená. Spoločnosť Accellion informovala, že bezpečnostný incident sa nezdá byť konkrétne zameraný na banku, a že boli ovplyvnení aj ostatní zákazníci služby zdieľania súborov FTA.

Z open-source projektu OpenWRT bol odcudzený zoznam používateľov fóra

Správcovia OpenWRT, open-source projektu, ktorý poskytuje bezplatný a prispôsobiteľný firmvér pre domáce smerovače, odhalili narušenie bezpečnosti. Tím OpenWRT uviedol, že zatiaľ čo útočník nebol schopný stiahnuť úplnú kópiu databázy, došlo k stiahnutiu zoznamu používateľov fóra, ktorý obsahoval osobné údaje, ako sú používateľské mená a e-mailové adresy. Uniknuté údaje nezahŕňali heslá. Správcovia OpenWRT upozorňujú používateľov fóra, že tiež môžu zaznamenať nárast pokusov o phishing v e-mailoch. Kompromitovanie účtu na fóre na OpenWRT by mohlo byť prvým krokom k eskalácii prístupu do interných sietí mnohých spoločností na vývoj hardvéru a softvéru.

Útočníci narušili certifikát, ktorý spoločnosť Mimecast vydáva na bezpečné pripojenie servera Microsoft 365 Exchange

Spoločnosť Mimecast, ktorá sa zaoberá bezpečnosťou e-mailov, zverejnila, že útočníci narušili jeden z certifikátov, ktoré spoločnosť vydáva zákazníkom na bezpečné pripojenie servera Microsoft 365 Exchange k ich službám. Aj keď nebol zverejnený presný počet zákazníkov, ktorí použili ukradnutý certifikát na zabezpečenie pripojenia slúžiaceho na synchronizačné úlohy cloudového servera Microsoft 365, Mimecast tvrdí, že bolo zasiahnutých zhruba 10 percent ich zákazníkov. Spoločnosť tvrdí, že v súčasnosti má viac ako 36 000 zákazníkov.

Útočníci zverejnili SQL databázu o veľkosti 70GB, ktorá obsahuje rôzne interné tabuľky obchodného reťazca Bonobos

Obchod s odevmi pre mužov Bonobos utrpel narušenie ochrany údajov. Útočník stiahol cloudovú zálohu ich databázy. Odhalil milióny osobných údajov zákazníkov tejto spoločnosti. Útočníci známi ako ShinyHunters, zverejnili celú databázu na bezplatné hackerské fórum. Zverejnený SQL súbor obsahujúci rôzne interné tabuľky dosahuje veľkosť 70GB. Záznamy sa líšia v závislosti od kategórie údajov. Zverejnené boli adresy a telefónne čísla pre 7 miliónov dodacích adries, informácie o účtoch pre 1,8 milióna registrovaných zákazníkov a 3,5 miliónov čiastočných záznamov o kreditných kartách. Spoločnosť sa vyjadrila, že útočníci nezískali prístup k interným systémom, ale len k záložnému súboru hosťovanému v prostredí externého cloudu.

Spoločnosť SonicWall sa stala obeťou útoku na jej interné systémy

Spoločnosť SonicWall, poskytovateľ internetovej bezpečnosti pre brány firewall a produkty VPN, zverejnila, že sa stala obeťou koordinovaného útoku na jej interné systémy. Spoločnosť uviedla, že útočníci zneužili zero-day zraniteľnosť v produktoch zabezpečeného vzdialeného prístupu SonicWall, ako sú

klient NetExtender VPN verzie 10.x a Secure Mobile Access (SMA), ktoré sa používajú na zabezpečenie vzdialeného prístupu používateľov k interným zdrojom.

Nový malvér FreakOut sa zameriava na linuxové zariadenia

Bol identifikovaný nový malvér s názvom FreakOut, ktorý sa zameriava na linuxové zariadenia, aby ich chytil do botnetu za účelom DDoS útokov a útokov na ťažbu kryptomien. Infikuje zariadenia, ktoré sú zraniteľné voči 3 chybám. FreakOut dokáže skenovať porty, vytvárať a odosielať dátové pakety, odpočúvať sieťovú prevádzku a podobne. Jednou zo zraniteľností, na ktoré sa zameriava, je CVE-2020-28188, čo je neoverené vzdialené vykonávanie príkazov v TerraMaster TOS. Druhou z nich je CVE-2021-3007, chyba deserializácie v Zend Framework, ktorá by mohla viesť k vzdialenému vykonávaniu kódu. Posledná je CVE-2020-7961, ktorá súvisí s deserializáciou na Liferay Portal verzie nižšej ako 7.2.1 CE GA2, ktorá by mohla viesť k vzdialenému vykonávaniu ľubovoľného kódu prostredníctvom webových služieb JSON (JSONWS).

Webový portal Teespring utrpel únik údajov, pričom zverejnený bol archív 7zip obsahujúci dva SQL súbory

Útočník odhalil podrobnosti o miliónoch používateľoch zaregistrovaných na webovom portáli Teespring, ktorý používateľom umožňuje vytvárať a predávať odevy s potlačou na mieru. Údaje Teespring boli sprístupnené ako archív 7zip, ktorý obsahuje dva súbory typu SQL. Prvý súbor obsahuje zoznam viac ako 8,2 milióna emailových adries používateľov Teespring a dátum poslednej aktualizácie emailovej adresy. Druhý súbor obsahuje podrobnosti o účtoch viac ako 4,6 milióna používateľov. Údaje zahrnuté v tomto SQL súbore sú hašovaná verzia emailovej adresy, používateľské meno, skutočné meno, telefónne číslo, adresa bydliska a identifikátor Facebooku a OpenID, ktoré používatelia používali na prihlásenie do svojich účtov.

V USCellular došlo k úniku niektorých osobných údajov

Prevádzkovateľ mobilnej siete USCellular utrpel únik údajov po tom, čo útočníci získali prístup k jeho systému CRM (customer retail management) a účtom zákazníkov. Z oznámenia nie je zrejmé, koľkých zákazníkov sa to týkalo a či boli zamestnanci napadnutí prostredníctvom phishingového e-mailu alebo iným spôsobom. Pri prezeraní účtu zákazníkov v systéme CRM by útočník mohol vidieť ich meno, adresu, PIN, čísla mobilných telefónov, plán služieb a fakturačné alebo zákaznícke výpisy. USCelluar uvádza, že čísla sociálneho zabezpečenia zákazníkov a informácie o kreditných kartách neboli prístupné, pretože sú maskované v systéme CRM.

Unikli údaje o viac ako 2,28 miliónov používateľoch zoznamovacej stránky MeetMindful.com

Útočník prezradil podrobnosti o viac ako 2,28 miliónov používateľoch zaregistrovaných na zoznamovacej webovej stránke MeetMindful.com, ktorá bola založená v roku 2014. Údaje zoznamky boli zadarmo zverejnené na verejne prístupnom hackerskom fóre s napadnutými databázami. Uniknuté dáta o veľkosti 1,2GB zahŕňajú mená, emailové adresy, bydlisko, rodinný stav, dátumy narodenia a podobne. Správy, ktoré si používatelia vymieňali, neboli obsiahnuté v uniknutom súbore.

- Spoločnosť Apex Laboratory potvrdila, že útočníci ukradli údaje o pacientoch počas útoku ransomvérom.
- Citrix vydal vylepšenie funkcií, ktoré má blokovať využívanie funkcie Datagram Transport Layer Security (DTLS) ako zosilňovací vektor pri DDoS útokoch.
- Spoločnosť TransLink potvrdila, že útočníci stojaci za ransomvérom Egregor, narušili jej sieť a potenciálne ukradli dáta o zamestnancoch.
- Viac ako 500 tisíc uniknutých údajov priradených k najlepším dvom desiatkam popredných herných spoločností je na predaj.
- Útočníci sa zameriavajú na používateľov kryptomien pomocou nového malvéru ElectroRAT.
- Viaceré úložiská kódov spoločnosti Nissan North America sa tento týždeň dostali na verejnosť po tom, čo spoločnosť nechala vystavený server Git chránený predvolenými prístupovými údajmi.
- Spoločnosť Dassault Falcon Jet utrpela únik údajov.
- Sieťový gigant Ubiquiti upozorňuje zákazníkov na potenciálny únik údajov.
- Google aj Apple zakázal aplikáciu Parler v obchode z dôvodu neodstraňovania príspevkov, ktoré podnecujú násilie v USA.
- Malvér v počítačoch Mac používa na vyhnutie sa analýze skripty AppleScripts určené iba na spustenie.
- Backdoor Sunburst vykazuje spoločné funkcie ako Kazuar, backdoor .NET, ktorý je predbežne prepojený s ruskou APT skupinou Turla.
- Nevydaný operačný systém Windows Core Polaris od spoločnosti Microsoft unikol online.
- Stránka SolarLeaks tvrdí, že predáva údaje odcudzené pri útokoch na SolarWinds.
- Hackeri zverejňujú údaje o vakcíne COVID-19, ktoré boli ukradnuté z agentúry pre lieky EÚ.

- **Odborníci odhaľujú útoky škodlivého softvéru proti kolumbijskej vláde a spoločnostiam.**
- **CISA vydala varovanie, že útočníci obchádzajú viacfaktorovú autentizáciu (MFA) a úspešne útočia na cloudové služby v rôznych organizáciách v USA.**
- **Facebook žaloval dvoch vývojárov doplnkov pre Chrome za extrakciu údajov z používateľských profilov - vrátane mien, ID používateľov a ďalších.**
- **Viac ako 10 miliónov používateľov si nainštalovalo aplikácie pre Android, ktoré zobrazovali reklamy mimo kontextu.**
- **Nezverejnená chyba servera Apache Velocity XSS má vplyv na webové stránky vlád.**
- **Linux Mint opravuje obchádzanie šetriča obrazovky, ktoré objavili dve deti.**
- **Joker's Stash, najväčšie internetové fórum kreditných kariet končí.**
- **FireEye vydal nový open-source nástroj v reakcii na kompromitáciu systémov SolarWinds.**
- **Spoločnosť MalwareBytes sa vyjadrila, že útočníci stojaci za útokmi na SolarWinds pristúpili k ich interným emailom.**
- **Útočník prezradil 1,9 milióna záznamov používateľov Pixlr obsahujúcich informácie, ktoré by mohli byť použité na vykonávanie cielených phishingových útokov.**
- **Útočník zverejnil databázu so 77 miliónmi záznamov používateľov Nitro PDF.**
- **Spoločnosť Intel zverejnila, že útočníci ukradli infografiku obsahujúcu informácie o finančných výsledkoch spoločnosti za štvrtý štvrťrok roku 2020 a za celý rok 2020.**
- **Severokórejskí útočníci sa prostredníctvom sociálnych médií zamerali na bezpečnostných výskumníkov.**
- **Ransomvér Fonix sa vypne a vydá hlavný dešifrovací kľúč.**

Závažné zraniteľnosti bežných softvérových produktov

Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu kritickej zraniteľnosti

Výskumný tím Eye Control objavil vo viac ako 100 000 zariadeniach Zyxel nebezpečnú zraniteľnosť. Zariadenia používané ako Firewall, VPN, alebo prístupový bod WLAN obsahujú „zadné vrátka“ vo forme účtu určeného pre inštaláciu aktualizácií firmvéru. Tento účet má administrátorské privilégiá a napevno nastavené prihlasovacie údaje.

V operačnom systéme ThinOS tenkých klientov Dell Wyse sa vyskytujú 2 kritické zraniteľnosti

V operačnom systéme ThinOS na zariadeniach Dell Wyse sa vyskytujú dve kritické zraniteľnosti, ktoré môžu viesť k vzdialenému vykonávaniu škodlivého kódu, prípadne k získaniu neoprávneného prístupu k ľubovoľným súborom. Zneužitím prvej zraniteľnosti je útočník schopný pristúpiť ku konfiguráciám. Druhá kritická chyba umožňuje nielen čítanie, ale aj zápis do konfiguračných súborov bez autentifikácie.

Kritická zero-day zraniteľnosť v Microsoft Windows Defender a ďalších desať v januárovom balíku opráv pre Windows

Spoločnosť Microsoft vydala januárové opravy pre operačné systémy Windows. V balíku 83 aktualizácií sa vyskytuje 11 kritických, z ktorých dve aktívne zneužívané sa nachádzajú vo Windows Defender a ovládači tlačiarní splwow64.exe. Umožňujú vzdialené vykonávanie kódu, falšovanie identity a zvýšenie privilégií.

Vážne zraniteľnosti open source softvéru Dnsmasq, ktorý používajú desiatky výrobcov sieťových prvkov

Tím JSOF zverejnil 7 zraniteľností nazvaných DNSpooq. Dnsmasq je open source softvér väčšinou zakomponovaný vo firmvéri sieťových prvkov od všetkých výrobcov. Dnsmasq slúži na preposielanie DNS požiadaviek nadradenému DNS serveru a následnú odpoveď ukladá do medzipamäte DNS, čím zrýchľuje komunikáciu na sieti a predchádza jej zahlcovaniu. Z aktuálne zverejnených 7 zraniteľností sú 4 zraniteľnosti pretečenia medzipamäte a 3 zraniteľnosti umožňujúce otravu záznamov v medzipamäti DNS.

Kritické zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero závažných zraniteľností a 6 kritických:
CVE-2021-1164: Zraniteľnosť v službe UPnP (Universal Plug and Play) smerovačov Cisco Small Business RV110W, RV130, RV130W a RV215W by mohla umožniť neoverenému vzdialenému útočníkovi vykonávať ľubovoľný kód alebo spôsobiť neočakávané reštartovanie dotknutého zariadenia.
CVE-2021-1138, CVE-2021-1140, CVE-2021-1142: Zraniteľnosti vo webovom používateľskom rozhraní softvéru Cisco Smart Software Manager Satellite môžu umožniť neautentifikovanému vzdialenému útočníkovi vykonávať ľubovoľný kód ako vysoko privilegovaný používateľ na dotknutom zariadení. Tieto chyby zabezpečenia sú spôsobené nedostatočnou validáciou vstupu.
CVE-2021-1264: Zraniteľnosť nástroja Command Runner v aplikácii Cisco DNA Center by mohla umožniť autentifikovanému vzdialenému útočníkovi injektovať príkazy. Je spôsobená nedostatočným overením vstupu.
CVE-2021-1300: Zraniteľnosť softvéru Cisco SD-WAN môže umožniť neautentifikovanému vzdialenému útočníkovi spôsobiť stav pretečenia medzipamäte. Zraniteľnosť je spôsobená nesprávnym spracovaním IP prenosu.

Mesačník zraniteľností Január 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
    - Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu kritickej zraniteľnosti
    - V operačnom systéme ThinOS tenkých klientov Dell Wyse sa vyskytujú 2 kritické zraniteľnosti
    - Kritická zero-day zraniteľnosť v Microsoft Windows Defender a ďalších desať v januárovom balíku opráv pre Windows
    - Vážne zraniteľnosti open source softvéru Dnsmasq, ktorý používajú desiatky výrobcov sieťových prvkov

https://www.csirt.gov.sk/aktualne-7d7.html?id=236