ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Apríl 2019

Vypracoval: CSIRT.SK

TLP: White

Pamätáte si ešte na váš život pred 15 rokmi? Facebook, e-shopy, online banking? Je až neuveriteľné, akým rozsiahlym vývojom a premenami prešiel náš digitálny život za toto pomerne krátke obdobie. V priebehu času sme vedome či nevedome zdieľali so svetom stále viac svojich osobných údajov. Na internet putovali naše identifikačné a zdravotné údaje, platobné a finančné dáta, prihlasovacie údaje do súkromných účtov, fotografie s geolokalizáciou, myšlienky a názory na diskusné fóra, či blogy. Internet však nie je bezpečné miesto a v tom istom období došlo k nespočetným prienikom a únikom databáz obsahujúcich rôzne citlivé dáta. Preston Hogue vo svojom článku opisuje, ako by si mohli útočníci vďaka niekoľkým veľkým únikom za posledných 10 rokov vytvoriť kompletnú digitálnu stopu náhodného amerického občana a poskladať si jeho život do nepríjemných detailov.

Len v minulom roku unikli miliardy záznamov, ako uvádzajú štúdie niekoľkých spoločností. Správa spoločnosti Identity Theft Resource Center hovorí o 1244 prienikoch do systémov (23% pokles oproti 2017) a 447 miliónov odcudzených osobných záznamov (126% nárast), pričom len polovica reportov uvádzala čísla. Spoločnosť Risk Based Security síce hovorí o miernom poklese oproti roku 2017, no čísla sú závratné – 6515 prienikov a takmer 6 miliárd uniknutých záznamov. V tomto prípade sa nejedná len o osobné záznamy. Štatistika spoločnosti 4IQ je však ešte desivejšia. Hovorí o takmer 12 500 potvrdených prienikoch a 424% náraste oproti roku 2017.

V súčasnosti sa objavujú nové druhy ilegálnych internetových obchodov, ktoré sa špecializujú na digitálne stopy obetí ako službu ponúkanú k uniknutým platobným údajom z kreditných kariet, ktoré predávajú iné nelegálne obchody. To umožňuje zločincom dostatočne dôveryhodne imitovať skutočných vlastníkov kreditných kariet, a tak obchádzať ochranné systémy finančných inštitúcií. Finančný sektor je zároveň najviac postihnutý automatizovanou aktivitou škodlivých botov. Podľa štúdie spoločnosti Distil Research Lab predstavujú ich dopyty takmer polovicu sieťovej aktivity smerujúcej na webové služby tohto sektoru.

Aspekty, ktorými ako používatelia útočníkom zjednodušujeme prácu, sú nepozornosť a nedbalosť. Aj preto spoločnosť Kaspersky minulý rok zaznamenala vyše 58 000 inštalácií rôzneho sledovacieho malvéru na zariadeniach Android svojich používateľov. Tento druh malvéru dokáže exfiltrovať širokú škálu osobných údajov, od hovorov a správ, cez kontakty a bankové údaje až po polohu používateľa. Do výpočtových zariadení používateľov sa malvér a útočníci ľahko dostávajú vďaka zanedbávaniu bezpečnostných aktualizácií nainštalovaného softvéru. Spoločnosť Avast odhadla na vzorke 163 miliónov počítačov, že až 55% programov na Windowsových inštaláciách je zastaraných a zraniteľných. Najmenej aktualizované softvéry sú Adobe Shockwave, VLC Media Player a Skype, pričom neaktualizovaných je vyše 94%. Problémové sú tiež Java JRE, 7-Zip, Foxit Reader a Microsoft Office, z ktorého ešte 15% inštalácií predstavuje dva roky nepodporovaná verzia Enterprise 2007.

Ďalším aspektom napomáhajúcim útočníkom v značnej miere je tvorba a používanie hesiel v praxi. Štúdia spoločnosti Harris Poll na vzorke 3000 respondentov ukázala, že len 39% používateľov tvorí heslá s použitím zmesi písmen, čísel a znakov a len 23% verí, že dĺžka hesla hrá dôležitú rolu. Len 32% dokázalo správne popísať, čo je to phishing, manažér hesiel a dvojfaktorová autentifikácia, zatiaľ čo

19% nedokázalo popísať ani jeden z týchto pojmov. K tomu ďalšia štúdia ukázala, že milióny ľudí stále okrem mien svojich zvieratiek a výročných dátumov používajú heslá ako 123456, qwerty, password, či 1111111.

Skvelým zdrojom citlivých dát sú podľa štúdie University of Hertfordshire tiež USB kľúče a iné úložné médiá kúpené z druhej ruky. Okrem vysokej šance, že sa na nich nachádza malvér existuje vysoká pravdepodobnosť, že predchádzajúci majiteľ svoje dáta zmazal nevhodným spôsobom a môžu byť jednoducho obnoviteľné, prípadne sa vôbec neunúval mazať ich. Výskumníci tak okrem iného našli fotky nahého muža, fotky vojaka a ľudí so zbraňami, daňové dokumenty, burzové prevody a laboratórne správy petrochemickej spoločnosti.

Pochybenie je však často aj na strane spoločností, ktoré nesprávnou konfiguráciou vystavia svoje databázy s dátami klientov internetu. Napríklad len v prvom kvartáli 2019 spôsobili nezabezpečené databázy čínskych firiem únik 590 miliónov životopisov.

Čo teda robiť, aby sme útočníkom neuľahčovali prístup k našim citlivým osobným dátam? Spoločnosť McAfee radí:

- Na sociálnych sieťach a vo svojich účtoch
  - Nastavte si súkromie a bezpečnosť, nenechávajte informácie, fotky, polohu a podobne verejné.
  - Aktivujte si dvojfaktorovú autentifikáciu
  - Používajte silné a originálne heslá, používajte manažér hesiel
  - Nepoužívajte svoje skutočné meno ako používateľské meno, aby ste neboli „vygoogliteľní“
  - Pred zdieľaním a komentovaním si premyslite, čo táto akcia o vás prezradí tretím stranám
  - Ak používate cloudové riešenie, implementujte dodatočné bezpečnostné opatrenia pre prístup k vašim dátam
- Nenaleťte podvodníkom a phishingu
  - Dávajte pozor kam klikáte, vyvarujte sa podozrivým linkom a neznámym vyskakovacím oknám
  - Dávajte pozor na podvodné dokumenty s gramatickými chybami, všeobecným pozdravom a nekvalitnou grafickou stránkou
  - Nevypĺňajte kvízy a „zábavné“ dotazníčky na sociálnych sieťach – často sa jedná o pokus nepozorovane vytiahnuť viac informácií o obeti
  - Nakupujte online rozumne, nenaleťte na príliš dobre vyzerajúce ponuky a berte do úvahy reputáciu obchodov

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci apríl riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Okrem toho sa naďalej venoval systému eID. Vyskytol sa tiež incident v súvislosti s portálom Slovensko.sk.

CSIRT.SK vykonal niekoľko vyžiadaných externých penetračných testov webových aplikácií a inštitúcií vo svojej konštituencii.

V rámci osvetovej a vzdelávacej aktivity prednášal člen tímu CSIRT na Fakulte matematiky, fyziky a informatiky UK v Bratislave o kryptoanalýze mobilnej šifry A5/1 a výzvach RSA algoritmu. Prezentácie k týmto prednáškam sú dostupné na našom webe.

Významné útoky vo svete

Tisíce nezabezpečených a zastaraných verzií analytickej platformy Kibana ponechávajú svoje Elasticsearch databázy nechránené a dostupné z internetu.

Anonymný bezpečnostný výskumník upozornil na výskyt vyše 26 000 inštancií analytickej platformy Kibana ponechaných dostupných voľne na internete. Kibana je platforma na spracovanie dát z Elasticsearch databáz. Jednou z konfiguračných chýb je práve ponechanie vzdialeného prístupu k nej, bez zabezpečenia heslom. Výskumník objavil pestrú paletu dát od veľkých spoločností, ako nešpecifikovaného výrobcu kamier (dáta ku každému vyrobenému kusu), či ázijskej akciovej burzy. Ďalším dôvodom na obavy je fakt, že väčšina skúmaných inštancií nebola aktualizovaná a obsahovala vážne zraniteľnosti.

Vyše 13 000 dátových úložísk a NAS zariadení voľne prístupných z internetu. Majitelia nenakonfigurovali autentifikáciu v iSCSI protokole.

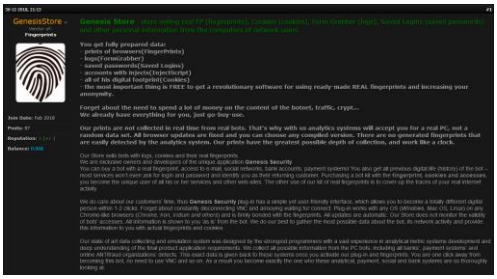
Nielen databázy, ale aj dátové úložiská nechávajú ľudia voľne prístupné z internetu. Vyše 13 000 iSCSI úložísk bolo objavených ponechaných bez potreby autentifikácie z dôvodu konfiguračných chýb. Náhodní útočníci tak môžu voľne sťahovať a mazať uložené súbory, no napríklad tiež nahrávať malvér a zadné dvierka do záloh systémov.

Dve verejne prístupné databázy na serveroch Amazonu exponovali používateľské mená, komentáre a heslá používateľov Facebooku, spolu vyše 540 miliónov záznamov.

Dva súbory dát používateľov Facebooku exponovali na internet citlivé údaje stoviek miliónov osôb. Jeden patril mexickej spoločnosti Cultura Colectiva a obsahoval 540 miliónov záznamov vrátane like-ov, komentárov a používateľské mená a podobne. Druhý patril aplikácii At the Pool a obsahoval okrem iného heslá vo voľnom texte 22 000 používateľov. Facebook kontaktoval prenajímateľa serverov, spoločnosť Amazon, so

žiadosťou o odstránenie databáz, hneď ako sa o incidente dozvedel. Databázy boli následne zabezpečené.

Kyber-zločinci predávajú úplné digitálne odtlačky vyše 60 000 osôb.



Nový kriminálny online obchod Genesis ponúka na predaj kompletné digitálne profily vyše 60 000 osôb. Obsahujú prihlasovacie údaje do online platobných portálov či internet bankingu, sociálnych sietí, súbory cookies súvisiace s týmito účtami, údaje z internetového prehliadača, signatúry WebGL a HTML5 canvas, a podobne. Takéto komplexné dáta obetí pomáhajú zločincom obchádzať bankové systémy proti podvodom. Identity obetí sa predávajú od 5 do 200 USD.

Výskumníkom sa podarilo zmanipulovať CT snímky priamo pri vyšetrení.

Výskumníci z izraelských Ben-Gurion Univeristy a Soroka University Medical Center vyvinuli malvér, ktorý dokázal v reálnom čase zmanipulovať CT snímky na ceste od skeneru do zobrazovacieho zariadenia. Malvér odstránil či pridal do snímok známky rakoviny, pričom lekári nerozoznali falošné snímky od pravých (úspešnosť bola 1-6% pokiaľ lekári nevedeli o manipulácii a 13-40% keď o manipulácii snímok vedeli). Výskumníci pri vývoji malvéru použili metódy strojového učenia.

Podvodníci stále využívajú schému Sextortion. Svoje e-maily vylepšujú tak, aby obišli anti-spam ochranu.

Sextortion je podvodná kampaň spamových e-mailov, v ktorej sa útočníci snažia obete presvedčiť, že sa nabúrali do ich počítačov a mailových účtov, nahrali ich cez webkameru v intímnej chvíli pri sledovaní pornografického materiálu a tieto nahrávky zverejnia pokiaľ obete nezaplatia požadovanú sumu. Celý príbeh

je vymyslený, aj keď môže pôsobiť dôveryhodne, nakoľko útočníci získali mohli získať nejaké informácie (napríklad k e-mailovým účtom) zo starých únikov. Táto schéma však v posledných mesiacoch začala strácať na lukratívnosti (takmer 10-násobný pokles ziskov útočníkov). Preto museli podvodníci zvoliť inú taktiku. Začali používať niekoľko trikov na oklamanie antispamovej ochrany a tiež do mailov pridali link na „ukážku“ nahratého videa, ktoré je však v zaheslovanom archíve .zip. Za heslo pýtajú 50 USD s vedomím, že tak presvedčia obete oveľa ľahšie, aby zaplatili aspoň túto menšiu sumu.

Správa okresu Garfield County, Utah, spracovávala administratívu papierovo po útoku ransomvérom.

Garfield County

Dôvodom úspechu útoku ransomvérom na miestnu správu okresu Garfield County v americkom štáte Utah bolo pravdepodobne kliknutie na phishingový link. Útočníci tak získali prístup do systémov správy, kde zašifrovali dôležité dáta. Samospráva musela na nejakú dobu prejsť na papierovú administráciu. Súbory boli obnovené po zaplatení výkupného.

Útočníci mali 3 mesiace prístup k e-mailovým účtom používateľov služieb Outlook.com, Hotmail, MSN spoločnosti Microsoft.

Microsoft

Neznámi útočníci získali na začiatku roka 2019 prístup k e-mailovým službám spoločnosti Microsoft (Outlook.com, Hotmail a MSN) na tri mesiace. Vektorom útoku bol servisný účet zamestnanca, ku ktorému získali prihlasovacie údaje. Spoločnosť informovala, že útočníci získali prístup k štruktúre zložiek v schránkach používateľov, predmetom e-mailov a menám a e-mailovým adresám adresátov, no nie k obsahu správ, ani prihlasovacím údajom. Toto tvrdenie však bolo spochybnené. Po tomto prieniku sa očakáva zvýšený výskyt phishingových útokov na používateľov kompromitovaných schránok.

Exponované osobné údaje vyše 100 miliónov používateľov JustDial z Indie kvôli nezabezpečenej databáze.

Bezpečnostný výskumník Rajshekhar Rajaharia informoval, že databáza údajov používateľov vyhľadávacej služby JustDial je verejne vystavená do internetu kvôli voľne dostupnej API. Hocikto tak mohol získať prístup k údajom vyše 100 miliónov osôb, vrátane ich mien, telefónnych čísel, e-mailových a domácich adries, fotografií, dátumu narodenia a povolania.

Phishing na banku Chase žiada od obetí okrem prihlasovacích údajov aj selfie.

Zaujímavá phishingová kampaň mieriaca na banku Chase si okrem prihlasovacích údajov do bankového účtu a e-mailu obete, fakturačnej adresy a údajov o kreditnej karte pýtala od obetí aj selfie s občianskym, alebo vodičským preukazom a fotky oboch strán týchto dokladov. Útočníci tak mohli získať kompletné údaje potrebné pre predstieranie online identity obetí. To mohli využiť napríklad pre získanie prístupu, či vytváranie nových účtov na hazardné stránky, burzy kryptomien, či stránky určené na prevody peňazí.

- **Odcudzenie údajov z asi 2 miliónov platobných kariet z PoS terminálov desiatok reštaurácií vlastnených Earl Enterprises.**
- **Rusko obvinené z falšovania signálu z navigačných družicových systémov (GPS, GLONASS,...)**
- **Medicínske záznamy 12,5 milióna tehotných žien z Indie ponechané exponované na internete.**
- **Spyware Exodus sa šíril pomocou 25 aplikácií pre Android cez Google Play.**
- **Hlavné mesto štátu New York, Albany, utrpelo škody spôsobené ransomvérovým útokom.**

- Prienik do databázy študentov a zamestnancov The Georgia Institute of Technology zasiahol 1,3 milióna osôb.
- Spoločnosť Bayer sledovala rok aktivitu malvéru na svojej sieti, za útočníka označila skupinu Winnti.
- Malvér na webstránke AeroGrow kradol 4 mesiace zákazníkom údaje o platobných kartách.
- Výskum spoločnosti Symantec ukázal, že dve tretiny z 1500 hotelov v 54 krajinách používa rezervačné systémy umožňujúce prístup k osobným údajom hostí a zrušenie ich rezervácie.
- Desiatky tisíc automobilov sprístupnila zlodejom mobilná aplikácia MyCar kvôli pevne naprogramovaným prihlasovacím údajom.
- Máte Alexu a nechcete byť odpočúvaní zamestnancami spoločnosti Amazon? Zrušte nastavenie povolenia v „Manage how your data improves Alexa“.
- Podľa spoločnosti Kaspersky vzrástol za dva roky podiel útokov na produkt Microsoft Office 4-násobne. Predstavuje 70% útokov detegovaných spoločnosťou.
- Pokuta 400 000 GBP pre tehotenský klub Bounty UK Limited za protizákonné zdieľanie a predaj osobných údajov 14 miliónov osôb.
- Ďalšie osobné údaje 65,5 miliónov osôb na predaj na darkwebe po únikoch vo februári a marci.
- Únik mien, domácich adries a e-mailových kontaktov tisícok zamestnancov FBI a pridružených organizácií.
- Google zdieľa lokalizačné dáta s políciou v rámci vyšetrovania trestných činov.
- Kybernetické útoky na niekoľko oddelení ukrajinskej armády. Spear phishing šíril malvér na vzdialený prístup k infikovaným zariadeniam.
- Pol miliardy relácií ukradnutých cez zraniteľnosti v pop-up blockeri pre prehliadač iOS Chrome. Užívatelia presmerovaní cez falošnú reklamu na škodlivé stránky využívané na phishing a šírenie malvéru.
- Útoky na klientelu IT consultingovej firmy Wipro Ltd. cez kompromitovanú sieť spoločnosti. Pravdepodobne útočila niektorá APT skupina.

TLP: White

- **Pokus o podvodné presmerovanie platieb zdravotnej poisťovne Blue Cross v Idahu viedol k úniku osobných údajov 5600 poistencov.**

- **Spoločnosť Navicent Health utrpela prienik do svojich systémov. Osobné údaje takmer 280 000 klientov v rukách útočníkov.**

- **Od začiatku roka 2017 prebieha neznámym štátom sponzorovaná kampaň útokov využívajúcich DNS presmerovanie. Zasiahnutých bolo 40 spoločností v 13 krajinách Stredného východu a severnej Afriky.**

- **Facebook ukladal heslá miliónov používateľov Instagramu v čitateľnej forme.**

- **Osobné údaje 300 000 iránskych vodičov verejne dostupné v nezabezpečenej databáze aplikácie Tap30.**

- **Výpadok stanice The Weather Channel na 90 minút po útoku ransomvérom. Personál obnovil IT systémy zo záloh.**

- **Prienik do databázy pensylvánskej kliniky pre liečbu závislostí. Unikli osobné údaje, ktoré sa dajú osobne priradiť vyše 146 000 pacientom.**

- **Únik citlivých údajov texaskej zdravotníckej spoločnosti EmCare patriacej Envision Healthcare zasiahol 60 000 osôb. Polovica z nich sú pacienti.**

- **Prienik do systémov Bodybuilding.com bol spôsobený pravdepodobne reakciou na phishingový e-mail.**

- **Nezabezpečená databáza pre Android aplikáciu WiFi Finder umožňovala prístup k 2 miliónom párov mien a hesiel vo voľnom texte pre prístupové body Wi-Fi.**

- **V prvom kvartáli 2019 vzrástol počet útokom ransomvérom na komerčné spoločnosti o 500%.**

- **Skupina MageCart kradla údaje z platobných kariet malvérom umiestneným na stránke amerického basketbalového tímu Atlanta Hawks.**

- **Webhostingová spoločnosť GoDaddy zrušila vyše 15 000 podvodných webstránok umiestnených na jej kompromitovaných kontách a obetiam prienikov resetovala heslá.**

- **Hong Kongská pobočka Amnesty International napadnutá pravdepodobne čínskou APT skupinou.**

- **Únik citlivých prihlasovacích údajov z databázy Docker Hub zasiahol približne 190 000 používateľov. Unikli aj prístupové tokeny pre GitHub a Bitbucket.**

- **Nezabezpečená databáza vystavovala internetu citlivé údaje vyše 80 miliónov amerických domácností.**

Závažné zraniteľnosti bežných softvérových produktov

Masívny útok na zariadenia značky ASUS

Spoločnosť Kaspersky odhalila masívnu kampaň zatiaľ neidentifikovanej APT skupiny zameranú na kompromitáciu zariadení ASUS na dodávateľskej úrovni. Na server spoločnosti nahrala upravenú verziu aplikácie ASUS Live Update obsahujúcu zadné dvierka. Cieľom bolo približne 600 zariadení identifikovaných podľa MAC adries, na ktoré bol v druhej fáze inštalovaný malvér. Odporúča sa overiť možnosť kompromitácie notebookov značky ASUS pomocou nástroja spoločnosti Kaspersky, alebo zoznamu cieľových MAC adries.

Aplikácia Signal - zraniteľnosť Homograph Domain

V aplikácii pre bezpečnú komunikáciu Signal existuje zraniteľnosť pri nedostatočnom overovaní používateľských vstupov, ktorá dovoľuje zneužiť homografy pri registrovaní podvodných domén a presvedčiť tak obeť, že pristupuje na legitímnu webstránku.

Kritické zraniteľnosti CMS Magento

V populárnom CMS Magento bolo opravených 37 zraniteľností, z ktorých štyri boli označené ako kritické a štyri ako závažné. Umožňujú vykonávať XSS a CSRF útoky, vzdialene vykonávať kód, či manipulovať s databázou webstránky pomocou SQL injekcie. Útočník môže získať citlivé údaje vrátane administrátorských prístupov a prevziať kontrolu nad stránkou.

Kritická zraniteľnosť na serveri Apache dovoľuje vykonávať kód

Kritická zraniteľnosť v aplikácii Apache server umožňuje vďaka dedeniu práv procesov zvýšiť útočníkom práva až na root a tak vykonávať kód. Nebezpečná je najmä pre služby poskytujúce webový hosting, nakoľko útočník môže

kompromitovať hostované webstránky. Zraniteľnosť je zneužiteľná na Unixových systémoch.

Zero-day na TP-Link Smart Home Router

Zero-day zraniteľnosť v routeroch TP-Link SR20 umožňuje útočníkom vykonávať ľubovoľný kód. Súvisí s procesom TDDP, ktorý zvyčajne beží s právami root. Zneužiť je ju možné cez lokálnu sieť. Zatiaľ neexistuje opravná aktualizácia.

WPA3 - nechránené WI-FI heslá

Kvôli nedostatkom vo WPA3 protokole dokážu útočníci zistiť heslá wi-fi siete a odpočúvať komunikáciu medzi zariadeniami pripojenými na danej sieti. Takto môžu získať čísla kreditných kariet, heslá, čítať správy a emaily, a pristupovať k ďalším odoslaným citlivým informáciám.

Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Aironet Access Points (CVE-2019-1826): nedostatočná sanitizácia používateľského vstupu v poliach wi-fi rámcov umožňuje vytvoriť DoS podmienky.
Cisco Nexus 9000 Series (CVE-2019-1590): kvôli nevhodnému overovaniu klientskych TLS certifikátov môže dochádzať k obchádzaniu autentifikácie a získaniu neautorizovaného prístupu k zariadeniu.
Cisco Umbrella (CVE-2019-1807): je možné prevziať kontrolu nad spustenou reláciou iného používateľa, nakoľko aplikácia nezneplatní predchádzajúcu otvorenú reláciu po prihlásení ďalšieho používateľa.
Cisco Web Secutiry Appliance (CVE-2019-1817): kvôli nevhodnej kontrole HTTP a HTTPS požiadaviek je možné odoslaním špeciálne vytvorených požiadaviek spôsobiť DoS podmienky.
Cisco Web Secutiry Appliance (CVE-2019-1816): nedostatočná sanitizácia používateľského vstupu vo webovom rozhraní a príkazovom riadku umožňuje útočníkovi lokálne injektovať príkazy s právami root.

Palo Alto Networks

Systém Palo Alto Networks PAN-OS mal zraniteľnosť CVE-2019-1572 umožňujúcu obchádzať autentifikáciu. Nachádzala sa v Management Web Interface a neprihlásený útočník sa mohol dostať k súborom PHP.

Mesačník zraniteľností Apríl 2019

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
    - Oracle Weblogic
    - Zraniteľnosti WPA3
    - TP-Link SHR
    - Apache
    - CMS Magento
    - Signal

https://www.csirt.gov.sk/aktualne-7d7.html?id=185