ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

November 2018

Vypracoval: CSIRT.SK

TLP: White

S blížiacimi sa vianočnými sviatkami sa nachádzame v nákupnej sezóne. Preto sa v novembrovej mesačnej správe pozrieme, na čo si pri online nákupoch dať pozor a ako sa pritom efektívne chrániť. Je totiž možné, že kyberzločinci využijú obdobie pred sviatkami podobným spôsobom, ako to urobili v novembrových dňoch Black Friday a Cyber Monday. V tom čase bolo jednoduchšie nachytať ľudí bažiacich po vysokých zľavách na podvodné ponuky a phishingové e-mailové kampane. Namiesto neuveriteľnej zľavy tak na webstránke, kam sa obeť cez podvodné ponuky preklikala, číhal útočník na jej platobné údaje. Neraz boli zneužité domény, ktorých majitelia si nepredĺžili ich prenájom. Útočníci ich rýchlo kúpili a vytvorili na nich falošné online obchody, napríklad so značkovým oblečením a obuvou, s lákavými cenami. Ich jediným cieľom bola krádež údajov o kreditných kartách, ktoré zadali pri pokuse o platbu ich nič netušiaci majitelia. Rozmohli sa aj tzv. „malvertising" kampane (spojenie slov „malware" a „advertising") ako nedávna masová kampaň cielená na zariadenia využívajúce iOS, a tiež prosby o dary falošným charitatívnym organizáciám. Americký US-CERT v danom týždni vydal varovanie podložené správou spoločnosti Zscaler, ktorá od polovice októbra do polovice novembra pozorovala stály nárast phishingových a spamových kampaní, v súhrne až 1,3 milióna.

Bežná rada, ako sa nestať obeťou phishingu, je kontrolovať, či prehliadač zobrazuje vedľa adresy webstránky „zelený zámok". V štúdii spoločnosti PhishLabs vyše 80% respondentov uviedlo, že zelený zámok pokladajú za známku legitímnej, či bezpečnej webstránky. Pritom sa nám tento piktogram len podáva informáciu, že naša komunikácia (odosielané a prijímané informácie) je šifrovaná, resp. že stránka používa HTTPS protokol. Tvorcovia phishingových domén sú však prispôsobiví a vynaliezaví, a tak v treťom kvartáli 2018 už 49% phishingových domén využívalo HTTPS, pričom len kvartál predtým to bolo 35%. O niektorých spôsoboch, ktoré útočníci na to využívajú, sme písali v minulomesačnej správe.

Zvýšil sa aj počet napadnutí legitímnych online obchodov malvérom MageCart, ktorý funguje ako softvérová čítačka kariet a odosiela útočníkom platobné údaje zadané do platobného rozhrania obchodu. Podrobnú spoločnú správu o fungovaní skupín MageCart vydali spoločnosti Flashpoint a RiskIQ. Situácia prerástla do takých rozmerov, že MageCart skupiny (napríklad MageCart skupina 3 a skupina 9) začali medzi sebou súperiť a vytláčať konkurenciu pozmeňovaním ňou zachytených platobných údajov. Tým ničia ich reputáciu u zákazníkov na darknete.

Pred útokom typu MageCart sa bohužiaľ ako zákazníci ubránime len veľmi ťažko, no existujú dobre fungujúce odporúčania, ktorých sa môžeme pri online nakupovaní držať.

- Ak chceme nakupovať u neznámeho obchodníka, preverme si jeho reputáciu online. Existuje obchod už nejakú dobu, alebo vznikol len nedávno? Pri novo vytvorených obchodoch je samozrejme oveľa vyššie riziko, že sa jedná o falošný obchod. Túto informáciu môžete zistiť napríklad pomocou nástroja WHOIS.
- Odporúča sa používať kreditnú kartu namiesto debetnej, aby vám v prípade podvodu útočníci nesiahli na vaše osobné konto. Tak aj v prípade, že vám banka stratu nahradí, nebudete mať

problémy s omeškaním platieb účtov a úverov. Využiť môžete aj služby spoločností poskytujúcich predplatené, rep. jednorazové virtuálne platobné karty.

- Pred kliknutím na reklamný odkaz e-shopu pozrieť v ľavom dolnom rohu prehliadača, či smeruje naozaj tam, kam hovorí. Po kliknutí skontrolovať doménu, v hornom odkazovom okne prehliadača, či sedí (napríklad pri prístupe na server Amazon bude v odkazovom okne www.amazon.com/... Spoločnosť vás nikdy nepresmeruje trebárs na doménu www.mojaevilstranka.com/...). Skontrolovať, či stránka využíva HTTPS protokol (zelený zámok v odkazovom okne) – no ako sme spomenuli vyššie, nestačí to.
- Väčšina spoločností (napríklad žiadna banková inštitúcia) vás nikdy nebude žiadať e-mailom, alebo telefonicky o vaše platobné, alebo prihlasovacie údaje. Ak vám príde správa, že ľubovoľný problém musíte urgentne riešiť, pretože inak hrozí zrušenie služby, ktorú využívate, zvýšte obozretnosť. Danú inštitúciu kontaktujte priamo – na telefónnom čísle či e-maile z faktúry, alebo ich oficiálnej webstránky, na ktorú ste pristúpili priamo, nie cez odkaz v e-maile. Na odkazy ani prílohy v e-maile neklikajte, aby ste predišli infekcii vášho zariadenia.
- Skontrolujte si cenu dopravy a dobu dodania. Niektoré obchody si kompenzujú nižšie ceny za tovar na poštovnom.
- Pravidelne kontrolujte výpisy z vášho účtu a prípadné nezrovnalosti bezodkladne hláste vašej banke.

Tím CSIRT.SK vám želá šťastné a veselé sviatky. No ostaňte ostražití, aby ste s vianočným pozdravom nestiahli aj nechcený darček vo forme malvéru.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci november riešil štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Nezaznamenal žiaden významný útok. Okrem toho dostal informáciu o druhom neúspešnom brute force útoku na e-mailové účty pracovníkov organizácie. Podobný útok na danú organizáciu sa odohral minulý mesiac.

CSIRT.SK vykonal niekoľko penetračných testov webových stránok a systémov inštitúcií vo svojej konštituencii.

V rámci penetračných testov v jednej organizácii analytici CSIRT.SK objavili prítomnosť vyše roka starej kritickej zraniteľnosti. Na základe tohto nálezu rozposlal CSIRT.SK svojej konštituencii varovanie s požiadavkou o kontrolu systémov a v prípade pozitívneho nálezu vykonanie nápravných opatrení.

V rámci prezentačnej a edukatívnej činnosti usporiadal CSIRT.SK jednodňový seminár v dvoch termínoch pre svoju konštituenciu. Na seminári predstavil svoje služby a kompetencie a informoval o povinnostiach inštitúcií vyplývajúcich zo zákona o kybernetickej bezpečnosti. Na seminári vystúpili aj hostia z Národného bezpečnostného úradu a Úradu podpredsedu vlády pre investície a informatizáciu.

V mesiaci november bol CSIRT.SK tiež účastníkom cvičenia Cyber Coalition, ktoré každoročne usporadúva aliancia NATO.

Významné útoky vo svete

Kampaň Emotet zbiera milióny e-mailových adries

Malvér Emotet začínal ako neveľmi úspešný bankový trójsky kôň. Neskôr ho však tvorcovia prebudovali na modulárny malvér určený na infiltráciu do systémov obetí, kam následne inštaluje ďalšie moduly a ďalší malvér, určený na rôzne účely, od krádeže informácií, cez RAT, po ransomvér. Dnes sa jedná o jeden z najpokročilejších botnetov. Najnovšie sa objavil podivný modul, ktorý z infikovaných systémov exfiltruje prijaté a odoslané e-maily za posledný polrok cez MS Outlook. Zatiaľ nie je jasné, čo je zámerom tvorcov, no v blízkej dobe sa dá očakávať nárast počtu prienikov do korporátnych systémov a únik citlivých dát.

Letecká spoločnosť Arik Air používala pre klientske dáta nezabezpečenú službu

Nigérijskej leteckej spoločnosti Arik Air unikli údaje zákazníkov z nevhodne nakonfigurovaného Amazon S3 úložiska. Výskumník zo spoločnosti Cloudflare, Justin Paine, z neho získal 994 CSV súborov s desiatkami tisíc riadkov z obdobia december 2017 – marec 2018. Unikli mená zákazníkov, e-mailové adresy, IP adresy z ktorých boli urobené nákupy a haše použitých kreditných kariet, no tiež prvých 6 a posledné 4 číslice kariet, identifikátory použitých zariadení, časy odletov a podobne.

Odhalená nová zraniteľnosť Facebooku

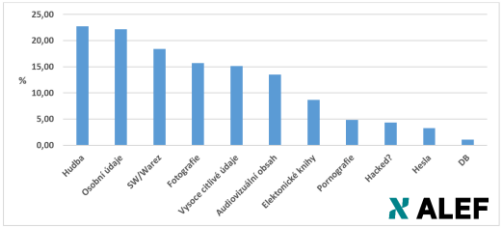
Bezpečnostný výskumník Philippe Harewood objavil na sociálnej sieti Facebook zraniteľnosť, ktorá umožňovala stať sa administrátorom ľubovoľného biznis účtu. Stačilo na to poslať http post požiadavku, ktorá obsahovala identifikátor spoločnosti, útočníkovho účtu a relácie. Nový administrátor by mal takto ľahký prístup ku všetkým nastaveniam biznis účtu, reklame, príspevkom a k možnosti pridávať a odoberať iných administrátorov.

TLP: White

Prienik do systémov banky HSBC

Útočníci prenikli do systémov spoločnosti HSBC a získali prístup k citlivým údajom klientov. Útok sa stal minulý mesiac medzi 4.-14.10. a bola pravdepodobne použitá technika „credential stuffing“, kedy útočník sa snaží použiť prihlasovacie údaje obete z iných služieb. Ak sa zhodujú, útok je úspešný. Preto odporúčame používať pre každú službu jedinečné heslo. Pri incidente unikli osobné údaje 1% amerických klientov, okrem iného číslo účtu, zostatok, história transakcií, dátum narodenia, adresa a telefonický a e-mailový kontakt. Spoločnosť zabezpečila svoje prihlasovacie rozhranie proti podobným útokom.

Citlivé údaje dostupné na CZ a SK webe



Bezpečnostní výskumníci z českého tímu ALEF CSIRT urobili prieskum, ako je to s dostupnosťou citlivých súborov cez automatické výpisy obsahu adresárov na webserveroch „Index of“ v českom a slovenskom internetovom priestore. Často sa totiž stáva, že administrátor so zámerne otvorenými adresármi sprístupní aj iné, ktoré nemal v úmysle zdieľať. Výskumníci využili internetové vyhľadávače, pričom po náročnej analýze objavili 185 webserverov s prístupnými citlivými dátami. Na 6 serveroch našli voľne dostupné heslá a 8 serverov obsahovalo informáciu o kompromitácii útočníkmi (1 z toho obsahoval viac ako 100 takých „vizitiek“). Na konci analýzy výskumníci upozornili majiteľov mnohých serverov na danú situáciu, pričom oslovení urobili nápravu.

Únik údajov hotelovej spoločnosti Radisson

Spoločnosť Radisson zastrešujúca vyše 1400 hotelov v 70 krajinách sveta utrpela prienik do svojich systémov, ktorý postihol „menej ako 10%“ členov programu „Radisson Rewards“. Unikli mená, adresy, e-mailové a telefonické kontakty, členské čísla a ďalšie informácie. Platobné dáta a heslá podľa spoločnosti neboli ohrozené. Útočníci sa do systémov dostali pravdepodobne cez zamestnanecké kontá, ktoré spoločnosť Radisson následne zabezpečila.

TLP: White

Veľký prienik do systémov FIFA

Po útoku skupiny Fancy Bear v roku 2017 utrpela futbalová asociácia FIFA ďalší prienik do svojich systémov. Útočníci na získanie prístupu pravdepodobne využili phishing. Asi 70 miliónov exfiltrovaných dokumentov sa dostalo na server Football Leaks, ktorý je akousi obdobou WikiLeaks. Analyzovať ich začalo 15 médií a 80 novinárov z 13 európskych krajín.

Krádež informácií austrálskej lodnej spoločnosti Austal

Austrálska lodná spoločnosť Austal, ktorá stavia lode aj pre americké a austrálske vojenské námorníctvo, zaznamenala útok na systémy svojej austrálskej vetvy. Útočníkom boli dostupné e-mailové a telefonické kontakty niektorých zamestnancov, no okrem toho sa im podarilo odcudziť interné dokumenty, za ktorých navrátenie požadovali výkupné. Spoločnosť odmietla vyjednávať.

Súkromné správy 81 000 Facebookových účtov na predaj

Na darknete sa objavil predajca FBSaler, ktorý predáva informácie zo 120 miliónov Facebokových účtov. Zároveň má prístup k súkromnej komunikácii 81 000 účtov. Cena za účet je 0,10$. Podľa spoločnosti Facebook sa útočníci k týmto dátam mohli dostať pomocou škodlivých modulov pre internetové prehliadače.

Bývalí zamestnanci Micron ukradli obchodné informácie za stovky miliónov dolárov

Byvalý prezident taiwanskej sekcie spoločnosti Micron, ktorý sa stal viceprezidentom taiwanskej konkurencie United Microelectronics Corporation so zmluvou o zdieľaní technológií s čínskou spoločnosťou Fujian Jinhua Integrated Circuit, najal dvoch zamestnancov Micron, aby pre neho získali technologické a obchodné tajomstvá spoločnosti. Títo odhadom exfiltrovali tajomstvá v hodnote 400 miliónov až 8,75 miliardy dolárov. Medzi uniknuté technológie patrí výrobný proces 25 nm DRAM, DRAM dizajn, alebo softvér na

sledovanie produktu počas výrobného procesu.

Polícia prelomila 258 000 šifrovaných telefónnych správ IronChat

Holandská polícia nešpecifikovanú dobu sledovala komunikáciu kriminálnikov cez aplikáciu IronChat, ktorá poskytuje možnosť šifrovania citlivých správ. Ako sa šifrovanie podarilo prelomiť, polícia nešpecifikovala. Vďaka zachytenej komunikácii bude možné obviniť a odsúdiť stovky zločincov. V tlačovom vyhlásení holandská polícia informovala, že zatiaľ zlikvidovala laboratórium na výrobu drog a zaistila hotovosť, automatické zbrane a veľké množstvo tvrdých drog.

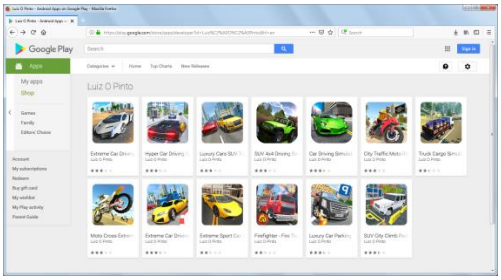
100 000 routerov v botnete kvôli starej zraniteľnosti

Výskumníci zo spoločnosti Qihoo 360 Netlab odhalili nový botnet, ktorý pomenovali BCMUPnP_Hunter. Od septembra napadol až 100 000 v USA, Indii a Číne, routerov od 116 výrobcov. Botnet zneužíva zraniteľnosť známu už od roku 2013. Jedná sa o zraniteľnosť vo firmvéri routerov Broadcom, ktorá však postihovala aj iných výrobcov. Veľké množstvo routerov však nebolo dodnes aktualizovaných. Botnet zneužíva tiež notoricky známy protokol UPnP určený pre jednoduchšiu komunikáciu medzi zariadeniami.

Desiatky miliónov automobilov pod útokom CarsBlues

Útok nazvaný CarsBlues ohrozuje desiatky miliónov automobilov na celom svete. Je možné ho vykonať s použitím bežne dostupného hardvéru a softvéru. Ak si majiteľ, či užívateľ vozidla (požičaného, firemného, a pod.) synchronizoval svoj telefón s automobilom, útočník môže zneužiť zraniteľnosť v bluetooth komunikácii a získať tak prístup ku kontaktom obete, logom a celým textovým správam. Obeť si pritom nič nevšimne. Útok môže prebehnúť po zapožičaní si vozidla, v autoservise, alebo keď sa hocijakým iným spôsobom dostane útočník k vozidlu. Najlepšou obranou je zmazať dáta pred udelením prístupu druhej osobe k vozidlu. Niektorí výrobcovia už vydávajú opravné aktualizácie.

Pol milióna inštalácií falošných aplikácií z Google Play



V depozitári softvéru pre telefóny využívajúce Android, Google Play, sa nachádzalo 13 falošných herných aplikácií. Tieto po nainštalovaní skryli svoju ikonu z plochy, čím vyvolali dojem, že inštalácia zlyhala. Následne v pozadí začali inštalovať aplikáciu Game Center, ktorú obete potvrdili v domnienke, že sa jedná o opakovanú inštaláciu hry. Táto aplikácia sa tiež po inštalácii ukryla a pri odblokovaní telefónu zobrazovala reklamy. Falošné aplikácie si nainštalovalo vyše 560 000 užívateľov, kým ešte boli v depozitári.

Americkej pošte unikli osobné údaje 60 miliónov občanov

Chybou v API aplikácie Informed Visibility, určenej na sledovanie pošty v reálnom čase, ponechala americká pošta USPS prístupné osobné údaje vyše 60 miliónov zákazníkov. Pred rokom spoločnosť o zraniteľnosti informoval nemenovaný bezpečnostný výskumník, no až na opakovanú výzvu v súčasnosti chybu odstránila. Za tú dobu však mali útočníci s používateľským účtom v službe prístup k osobným údajom miliónov zákazníkov, ako menám, telefonickým a e-mailovým kontaktom, adresám a podobne, ktoré navyše mohli meniť.

70 000 útokov mobilného spywaru

Za posledné tri mesiace došlo k napadnutiu vyše 70 000 mobilných zariadení bankovým trójskym koňom s ransomvérom Rotexy. Vyvinul sa zo spyware SMSThief a využíva tri komunikačné kanály – okrem klasického C2 centra je to SMS komunikácia a JSON komunikácia cez Google Cloud Messaging. Malvér obsahuje aj ďalšie pokročilé funkcionality. Obete nedávnych útokov pochádzajú najmä z Ruska, Ukrainy, Nemecka a Turecka.

Únik informácií 1,8 milióna používateľov nemeckej sociálnej siete Knuddels

1,8 milióna užívateľských mien a 808 000 e-mailových adries uniklo nemeckej flirtovacej sociálnej sieti Knuddels.de po úspešnom útoku. Jednalo sa o všetky účty užívateľov, ktorí si ich založili do 20 júla 2018. Vyše tretinu účtov spoločnosť vlastniaca webstránku overila a zvýšila bezpečnostné opatrenia. Vyšetrovanie však zistilo, že pred útokom spoločnosť nechránila citlivé dáta a napríklad heslá používateľov mala uložené vo voľnom texte. Spoločnosť dostala pokutu za porušenie ochrany osobných údajov v rámci regulácie GDPR len vo výške 20 000 eur, nakoľko ochotne spolupracovala a promptne riešila potrebné zabezpečenie.

Ukrajinský hacker za mrežami za infikovanie 2000 obetí malvérom typu RAT

42 ročný muž z Ukrajiny bol uväznený po tom, ako polícia našla dôkazy, že infikoval vyše 2000 obetí z 50 krajín sveta malvérom DarkComet typu Remote Access Trojan (RAT). Pomocou neho mohol vzdialene kontrolovať zariadenia obetí, sledovať ich činnosť, zaznamenávať stlačené klávesy a tak odchytávať heslá, inštalovať malvér, či kradnúť dokumenty.

Pokuta pre Uber za bezpečnostný incident

Holandské a Britské úrady uložili spoločnosti Uber pokutu v sume približne 900 000 libier za únik informácií v roku 2016. Spoločnosti unikli osobné údaje 7 miliónov vodičov a 57 miliónov cestujúcich kvôli „bezpečnostným problémom, ktorým bolo možné sa vyhnúť“. Unikli mená, telefonické a e-mailové kontakty a kópie vodičských preukazov. Namiesto oznámenia úniku spoločnosť zaplatila útočníkovi $100 000 za vymazanie údajov a mlčanlivosť.

Únik 2,65 milióna medicínskych záznamov po prieniku do systémov Atrium Health

Spoločnosť Atrium Health sa dozvedela o úniku citlivých dát svojich klientov zo systémov svojho platobného partnera AccuDoc Solutions. Útočníci ukradli dáta 2,65 milióna pacientov z obdobia 22.9-29.9.2018, ktoré zahŕňali mená, adresy, dátumy narodenia, informácie o zdravotnom poistení, zostatky na účtoch a čísla medicínskych záznamov. Okrem toho získali 700 000 čísiel sociálneho poistenia „Social Security“. Obe spoločnosti promptne reagovali, zabezpečili svoje systémy a informovali dotknutých klientov.

Ďalšia nezabezpečená databáza vystavila na verejnosť osobné údaje 57 miliónov Američanov a 27 miliónov firemných záznamov

Ďalší úlovok Boba Diachenka, známeho lovca nezabezpečených databáz. Je ním server ElasticSearch bez hesla, dostupný z internetu. Server vystavoval na verejnosť niekoľko databáz, pričom jedna z nich obsahovala osobné údaje 57 miliónov Američanov, zahŕňajúce mená, adresy, e-mailové a telefonické kontakty a IP adresy. Druhá, nazvaná „Yellow Pages“ obsahovala firemné údaje, spolu takmer takmer 27 miliónov záznamov, ktoré obsahovali mená, informácie o zamestnancoch, príjmy a mnohé údaje o spoločnosti. Javí sa, že tieto databázy sú spojené s kanadskou spoločnosťou Data&Leads. Diachenko poskytol údaje službe Have I Been Pwned, aby si potenciálne obete mohli overiť, či unikli aj ich údaje.

Útok EternalSilence a NSA malvér v 45 000 routeroch

Spoločnosť Akamai zaznamenala útok na routery v domácnostiach a malých spoločnostiach, ktorý technikou UPnProxy zmení nastavenia v NAT tabuľkách tak, aby bolo možné pristupovať k interným zariadeniam za routerom cez SMB port 139, alebo 445. Útok nazvala EternalSilence ako kombináciu názvu malvéru „EternalBlue“, ktorý unikol NSA a zneužíval zraniteľnosť SMB protokolu a názvu cookie „galleta silenciosa“, ktorý útočníci použili na prestavenie konfigurácie NAT na napadnutých routeroch. Spoločnosť zaznamenala vyše 45 000 routerov, do ktorých bol robený takýto zásah.

Prienik do systémov firmy DELL

Spoločnosť Dell zaznamenala v prvej polovici mesiaca na svojich systémoch pokus o exfiltráciu osobných údajov svojich zákazníkov. Útočníci sa pokúšali získať ich mená, e-mailové adresy a hašované heslá. Spoločnosť vyhlásila, že k úniku údajov vďaka včasnej detekcii pravdepodobne nedošlo a že platobné údaje neboli ohrozené. Pristúpila k zmene hesiel všetkých zákazníkov a povolala nezávislú firmu na vykonanie forenznej analýzy.

Desiatky miliónov zákazníkov v prístupnej databáze Sky Brazil a FIESP

Ďalší ElasticSearch server bez hesla, prístupný z internetu, dovoľoval prístup k osobným údajom 32 miliónov zákazníkov televíznej spoločnosti Sky Brazil. Údaje obsahovali okrem iného mená, adresy, dátumy narodenia, fakturačné údaje, šifrované heslá a telefonické a e-mailové kontakty. Ak by boli tieto dáta ukradnuté, bolo by napríklad možné postaviť na nich vysoko cielenú a efektívnu phishingovú kampaň.
Podobné nechcené sprístupnenie citlivých údajov 34,8 miliónov záznamov cez databázu ElasticSearch riešila tento mesiac aj brazílska spoločnosť FIESP, reprezentujúca 130 000 priemyselných spoločností.
ElasticSearch databázy boli podľa vývojárskej spoločnosti vyvinuté pre interné systémy, a teda nie sú určené pre servery vystavené do internetu.

Únik dát pol miliardy zákazníkov hotelovej spoločnosti Marriott

Hotelová spoločnosť Marriott zistila prienik do systémov svojej divízie Starwood, ktorý začal v roku 2014 (ešte pred akvizíciou spoločnosti Starwood) a trval do 10. Septembra 2018. Všetci zákazníci, ktorí si v tomto období rezervovali ubytovanie cez program Starwood Preferred Guest, sú týmto únikom postihnutí. Odhadom sa jedná o pol miliardy rezervácií. Útočníci si odosielali dáta zašifrované, aby ich neodhalili kontrolné systémy. Exfiltrovali údaje ako mená, adresy, telefonické a e-mailové kontakty, dátumy narodenia, čísla pasov, rezervačné údaje. Platobné údaje boli v systéme šifrované, no nie je isté, či sa útočníci nedostali aj k šifrovacím kľúčom.

Závažné zraniteľnosti bežných softvérových a hardvérových produktov

Zero-day zraniteľnosť vo VirtualBox umožňuje ovládnuť hostiteľský systém

Vo virtualizačnom nástroji VirtualBox od Oracle pri nastavení virtuálnej sieťovej karty existuje zraniteľnosť, ktorá umožňuje preniknúť z virtuálneho systému do hosťovského a následne s využitím ďalších metód eskalovať privilégiá až na úroveň systému. To dovoľuje napríklad vzdialene vykonávať kód.

Zraniteľnosť PHP funkcie imap_open umožňuje ovládnuť server

Funkcia imap_open dokáže pri nevhodnom kontrolovaní vstupov spúšťať shell príkazy na vzdialenom serveri, čo môže viesť k úplnému ovládnutiu servera.

Zraniteľnosti modulov WordPress umožňujú prevziať kontrolu nad webstránkou

Tri moduly CMS systému WordPress obsahujú kritické zraniteľnosti, ktoré umožňujú zvýšenie privilégií ľubovoľného užívateľského účtu, následne získať prístup do administrátorského účtu, a tak získať kontrolu nad celou webstránkou. Jedná sa o moduly WooCommerce, AMP a WP GDPR Compliance.

BleedingBit - kritické zraniteľnosti Bluetooth čipov v prístupových bodoch

Milióny wi-fi prístupových bodov a iných zariadení môžu byť ohrozené dvomi kritickými zraniteľnosťami nazvanými BleedingBit a prístupné k úplnému ovládnutiu útočníkom. Objavené zraniteľnosti sa nachádzajú v Bluetooth Low Energy (BLE) čipoch od spoločnosti Texas Instruments, ktoré sú využívané v prístupových zariadeniach pokrývajúcich až 70% korporátneho trhu.

Apache Struts obsahuje kvôli knižnici Commons FileUpload dva roky starú kritickú zraniteľnosť

Kritická zraniteľnosť knižnice Apache Commons FileUpload známa dva roky je stále prítomná v jednej z podporovaných verzií Apache Struts napriek tomu, že existuje opravená verzia knižnice. Zraniteľnosť môže viesť k vzdialenému vykonávaniu kódu a prevzatiu kontroly nad systémom. Knižnicu Commons FileUpload je potrebné nahradiť novou verziou ručne. Okrem Struts ju využívajú aj ďalšie aplikácie, preto je potrebná kontrola, či v systéme neexistujú ďalšie kópie zraniteľnej verzie.

Kritická zraniteľnosť Adobe Flash Player so zverejneným popisom

Adobe Flash Player obsahuje kritickú zraniteľnosť, ktorá umožňuje útočníkovi vzdialene vykonávať kód. Súvisí s chybou komponentu AVM, kedy tento pred použitím neoveruje typ objektu, ktorý mu bol zadaný. Informácie o zraniteľnosti boli zverejnené, preto sa odporúča bezodkladné odstránenie zraniteľnosti.

Zraniteľnosti Cisco

Spoločnosť Cisco opravila kritickú zraniteľnosť CVE-2018-15381 v softvéri Cisco Unity Express nachádzajúcu sa vo verziách starších, ako 9.0.6. Chyba deserializácie Java objektov umožňovala útočníkovi vykonávať ľubovoľné shell príkazy s root právami.
Kritická zraniteľnosť sa nachádza aj v produkte Cisco Stealthwatch Enterprise verzie 6.10.2 a staršie. Zraniteľnosť má označenie CVE-2018-15394 a útočníkovi umožňuje obísť autentifikáciu odoslaním špeciálne upravenej http požiadavky a získať tak v zraniteľnom systéme administrátorské práva. Existujú aktualizácie.
Kritická zraniteľnosť CVE-2018-15439 sa nachádza v produktoch Cisco Small Business Switches série 200, 250, 300, 350, 350X, 500 a 550X. Zariadenia za istých okolností umožnia neautentifikovanému vzdialenému útočníkovi vytvoriť si účet s administrátorskými právami bez informovania administrátorov. Existujú aktualizácie.
Cisco opravilo závažnú zraniteľnosť CVE-2018-0284 aj v sériách Meraki MR, MS, MX (aj virtuálne vMX100), Z1 a Z3. Chyba umožňuje útočníkom meniť konfiguračné súbory zariadení.
Aktualizácia je dostupná tiež pre kritickú zraniteľnosť CVE-2018-15441 v produkte Cisco Prime License Manager, ktorý nedostatočne sanitizuje užívateľský vstup pred jeho použitím ako SQL dotaz, a teda je v ňom možné vykonať SQL injekciu.

Zraniteľnosti VMware

Spoločnosť VMware opravila v niekoľkých svojich produktoch zraniteľnosť CVE-2018-6981, umožňujúcu vzdialene vykonávať kód, ak je povolená virtuálna sieťová karta „vmxnet3“. Zraniteľné produkty sú:
VMware Fusion 10.1.4, 11.0.1
VMware Fusion Pro 10.1.4, 11.0.1
VMware Workstation 14.1.4, 15.0.1
VMware Workstation Player 14.1.4, 15.0.1
VMware Workstation Pro 15.0.1
Vo vyššie uvedených produktoch bez špecifikácie verzie a v produkte VMware Esxi, ak je povolená virtuálna sieťová karta „vmxnet3“, existuje zraniteľnosť CVE-2018-6982 umožňujúca únik informácií z hostiteľského systému do hosťovského. Spoločnosť VMware vydala aktualizácie.
Oprava bola vydaná aj na zraniteľnosť CVE-2018-6980 v produkte VMWare vRealize Log Insight, ktorá umožňuje obísť autorizáciu pri registrácii používateľa.
V produkte VMWare vSphere Data Protection 6.0.9 a 6.1.10 existujú a boli opravené 4 kritické zraniteľnosti: CVE-2018-11066 (vzdialené vykonávanie kódu), CVE-2018-11076 (injekcia príkazov v rámci zraniteľnej aplikácie s root právami), CVE-2018-11077 (únik informácií cez VDP Java manažment, krádež súkromného kľúča a man-in-the-middle útok), CVE-2018-11067 (otvorené presmerovanie kvôli nedostatočnej sanitizácii užívateľského vstupu).

Mesačník zraniteľností November 2018

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
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java

6. Iné tohtomesačné závažné zraniteľnosti
    - Zraniteľnosti BleedingBit
    - Zraniteľnosti modulov WordPress
    - Zraniteľnosť PHP
    - Zero-day zraniteľnosť vo VirtualBox

https://www.csirt.gov.sk/aktualne-7d7.html?id=170