ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

August 2019

Vypracoval: CSIRT.SK

TLP: White

Sofacy, Fancy Bear, Tzar, Cozy Bear, Equation Group, Turla, Charming Kitten, Lazarus, Silence Group či Cloud Atlas. Počuli ste už niekedy tieto názvy? Označujú tzv. APT skupiny a akosi personalizujú číselné označenia týchto skupín. Napríklad APT28 – Sofacy/Fancy Bear. Skratka APT označuje tzv. Advanced Persistent Threat, čiže pokročilé perzistentné hrozby. V ľudskej reči sa jedná o skupiny útočníkov, ktoré štandardne platí a organizuje niektorý štát. Najznámejšie skupiny pracujú pre Rusko, Čínu, Irán, Severnú Kóreu, Saudskú Arábiu, Izrael, či štáty Five Eyes (USA, Kanada, Veľká Británia, Austrália, Nový Zéland). Majú čas, peniaze a prostriedky na plánovanie a prevádzanie útokov na ciele, ktoré sú pre daný štát zaujímavé. Najčastejšou motiváciou je získanie vojenských a politických tajomstiev iných štátov, či technológií a poznatkov. APT skupiny však vykonávajú aj sabotážne útoky a niekedy útoky so zámerom finančného zisku.

Činnosť APT skupín je možné sledovať pomocou nepriamych indícií. Bezpečnostní výskumníci napríklad využívajú rodiny malvéru, ktoré sú typické pre tú-ktorú skupinu. APT skupiny majú prostriedky na vývoj vlastného pokročilého škodlivého kódu, ktorý často unikne a začnú ho používať malí hráči na poli kybernetickej kriminality. Výskumníci využívajú aj stopy v kóde malvéru a štýl či rukopis, akým bol napísaný. V kóde sa môžu nachádzať popisky v materskom jazyku skupiny, informácie o geolokácii (napríklad vo forme časového pásma), používané súbory IP adries, či časové pečiatky. Podobné informácie však môžu byť podvrhnuté samotnými útočníkmi, aby zmiatli bezpečnostných výskumníkov a priviedli ich na falošnú stopu. Niektoré z najznámejších kúskov malvéru, ktorý používajú APT skupiny, sú

- Flame (zbierka útočných nástrojov Equation Group z NSA),
- Stuxnet (sabotážny nástroj použitý Izraelom a USA na zničenie centrifúg využívaných v iránskom jadrovom programe),
- Shamoon (kód na ničenie dát z Iránu),
- Winnti (modulárny trójsky kôň na tvorbu zadných vrátok v napadnutých systémoch vyvinutý a používaný čínskymi APT),
- Uroburos (rootkit pochádzajúci od ruskej skupiny Turla),
- WannaCry (neslávne známy ransomvér z dielne Severnej Kórei)
- NotPetya (ruský ransomvér použitý proti Ukrajine skupinou Fancy Bear)
- EternalBlue (exploit z dielne NSA, ktorý sa po svojom úniku stal kvôli svojej efektivite obľúbeným v ďalších APT skupinách aj u kybernetických kriminálnikov)

Tohtoročná správa Data Breach Investigations Report, ktorú uverejnila bezpečnostná spoločnosť Verizon hovorí, že najčastejším pôvodcom útokov a prienikov do systémov vo verejnej správe sú štátmi sponzorované skupiny (APT) vykonávajúce kybernetickú špionáž. Zaujímavý prehľad aktivít APT skupín vydáva pod názvom „APT trends report“ kvartálne spoločnosť Kaspersky. Odvoláva sa v nej aj na správy iných bezpečnostných spoločností. Okrem toho na svojom webe uverejňuje správy o aktuálnej činnosti rôznych APT skupín. Poďme sa teraz pozrieť na niektoré operácie APT skupín, o ktorých informovali médiá v auguste 2019.

Bezpečnostná spoločnosť Kaspersky monitorovala činnosť skupiny Cloud Atlas, ktorá už niekoľko rokov vykonáva kybernetickú špionáž vládnych a výskumných organizácií, no tiež priemyslu

a náboženských organizácií nachádzajúcich sa prevažne v Ázii a Východnej Európe. Spoločnosť spozorovala nasadenie nového polymorfného malvéru. Pôvod skupiny nie je známy, no pravdepodobne je ich materským jazykom ruština.

Kriminálna rusky hovoriaca skupina Silence APT primárne zameraná na štáty bývalého Sovietskeho zväzu viedla za posledný rok agresívnu kampaň proti bankám v 30 krajinách sveta v Amerike, Európe, Afrike a Ázii. Podľa bezpečnostnej spoločnosti Group-IB skupina prišla s vylepšenými útočnými nástrojmi a zvýšila frekvenciu útokov. Útočníci začali od mája používať loader Ivoke a niekoľko trójskych koní vrátane EmpireDNSAgent, Atmosphere a xfs-disp.exe. Päťnásobne zvýšila sumu odcudzených peňazí z 800 000 na 4,2 milióna USD. Útok na bankomaty bangladéšskej Dutch-Bangla Bank znamenal pre skupinu „zárobok“ vyše 3 miliónov USD. Ďalšie kampane boli zaznamenané v Indii (august 2018), Rusku (február a jún 2019), Kyrgyzsku (máj 2019), Čile, Ghane, Costa Rice, a Bulharsku (júl 2019).

Bezpečnostní výskumníci firmy Secureworks Counter Threat Unit objavili novú APT skupinu, ktorú pomenovali LYCEUM. Skupina sa zameriava na kritickú infraštruktúru krajín Blízkeho východu vrátane ropných a plynárenských spoločností. Pri útokoch využíva nový malvér určený na krádež prihlasovacích údajov, ktorý šíri pomocou spear-phishingových kampaní. Výskumníci pozorovali podobnosti v štýle útokov s iránskymi APT, no nedokázali tieto kampane jednoznačne priradiť niektorej známej skupine.

Čínska skupina APT41 operujúca na poli štátom sponzorovanej kybernetickej špionáže aj finančne motivovaného zločinu, ktorej cieľmi sa stali herné, zdravotné, technologické, telekomunikačné a turistické spoločnosti, no tiež vzdelávacie inštitúcie, útočila na nemenovanú americkú univerzitu. Informovala o tom bezpečnostná spoločnosť FireEye. Útok bol odhalený a zablokovaný pravdepodobne dostatočne včas na to, aby útočníci stihli exfiltrovať citlivé dáta. Skupina okrem iného využíva neverejný malvér určený na vedenie kybernetických špionážnych kampaní, čo u čínskych APT skupín nie je bežné.

Štáty zoskupenia Five Eyes sa zas vyjadrili proti zavedeniu end-to-end šifrovaniu v komunikačných aplikáciách, ktoré plánuje zaviesť spoločnosť Facebook a ktoré znemožňuje prístup k obsahu správ všetkým (vrátane Facebooku) okrem odosielateľa a príjemcu správy. Hlavným dôvodom nesúhlasu bola nemožnosť prístupu k obsahu autoritami pri vyšetrovaní závažných trestných činov. Zoskupenie žiada vytvorenie zadných vrátok. To by však predstavovalo bezpečnostnú dieru, ktorú by mohli ľahko zneužiť kriminálnici. Či by samotné vlády Five Eyes pristupovali k obsahu súkromných správ svojich občanov len v legitímnych prípadoch počas vyšetrovaní, sa môžeme len domnievať.

Bezpečnostní výskumníci sledujú činnosť a zbierajú informácie o APT skupinách. Informácie tiež medzi sebou zdieľajú. Vďaka tomu je možné zostavovať profily týchto nebezpečných skupín, pochopiť ich taktiku a spôsoby útokov a tvoriť účinnejšiu obranu proti ich aktivitám.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci august riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Okrem toho CSIRT.SK pokračoval v riešení jedného ransomvérového útoku na dátové úložiská. CSIRT.SK prijal tiež hlásenie zraniteľnosti spojenej s nesprávnym overovaním elektronického podpisu jednej aplikácie. Dodávateľ chybu odstránil.

V rámci proaktívnej činnosti varoval CSIRT.SK svoju konštituenciu pred kritickou zraniteľnosťou RDP protokolu operačných systémov Windows s názvom BlueKeep.

CSIRT.SK vykonával niekoľko vyžiadaných externých penetračných testov inštitúcií vo svojej konštituencii.

V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia CSIRT.SK zúčastnili na niekoľkých vzdelávacích a certifikačných podujatiach a konferenciách.

Významné útoky vo svete

Nezabezpečená Elasticsearch databáza voličov vystavená do internetu poskytovala prístup k osobným údajom 80% čílskej populácie.

Výskumníci spoločnosti Wizcase objavili nezabezpečenú databázu obsahujúcu osobné údaje vyše 14,3 milióna občanov Čile, vrátane vysokopostavených funkcionárov. Toto číslo predstavuje 80% populácie štátu. Databáza Elasticsearch obsahovala mená, adresy, pohlavie, vek a daňové identifikačné čísla. Vlastník servera s databázou je neznámy a údaje pravdepodobne zozbieral z oficiálnych stránok čílskej volebnej agentúry.

Phishingová kampaň na amerických dodávateľov energií spájaná s APT skupinou.

Americké energetické firmy sa stali obeťou útokov APT skupiny, ktorá sa snažila o prienik do ich systémov pomocou phishingovej kampane. V nej predstierala správy licenčnej rady US National Council of Examiners for Engineering and Surveying, v ktorých sa hovorilo o tom, že spoločnosť neprešla skúškami. Škodlivé správy obdahovali dokument MS Word s makrami, ktoré na zariadenie obete mali stiahnuť škodlivý kód vo formáte .txt, ktorý sa dekódoval a premenil na .exe a .dll súbory. Útočníci využívali malvér typu RAT s názvom LookBack. Spoločnosť Proofpoint spojila útoky so (pravdepdobne) čínskou skupinou APT10, Menupass, ktorá útočila aj na Japonské firmy.

Americké školy v okrese Houston, Alabama, museli dvakrát posunúť zahájenie školského roka kvôli útoku ransomvérom.

Školy v okrese Houston v americkom štáte Alabama museli dvakrát v priebehu týždňa posunúť začiatok školského roka. Nový naplánovaný dátum bol 12.8.. Dôvodom bol ransomvérový útok, ktorý znefunkčnil školskú infraštruktúru vrátane 4000 počítačových systémov a telefónnej siete. Všetky tieto systémy bolo potrebné obnoviť zo záloh.

Nesprávne nakonfigurované JIRA servery umožňujú prístup k citlivým interným informáciám mnohých spoločností, vrátane skupiny Fortune 500.

Bezpečnostný výskumník Avinash Jain informoval o skutočnosti, že konfiguračné chyby v projektovej manažovacej platforme JIRA spôsobili exponovanie citlivých informácií stoviek firiem do internetu. Prístupné boli údaje o zamestnancoch a ich kompetenciách, tajné projekty a identifikačné údaje. Mnoho z poškodených firiem sa nachádza v zozname Fortune 500 a poškodené boli aj vládne organizácie.

Masívna ransomvérová kampaň zasiahla 23 vládnych organizácií v americkom Texase.

Koordinovaná masívna kampaň postihla aspoň 23 vládnych organizácií v americkom štáte Texas. Podľa indícií v nej bol zainteresovaný ten istý útočník. Autority, ktoré prípad vyšetrovali, neuviedli podrobnosti, ktoré organizácie boli zasiahnuté, z dôvodov vyšetrovania. Informovali však, že systémy štátu Texas neboli útokom zasiahnuté.

Spoločnosť Twitter zrušila vyše 200 000 účtov spojených s čínskou vplyvovou kampaňou zameranou na protesty v Hong Kongu.

Protesty v Hong Kongu nezostali bez odpovede čínskej strany. Spoločnosť Twitter vystopovala čínsku kampaň ku dvom falošným účtom, ktoré predstierali príslušnosť k hongkongským médiám a vykresľovali protestujúcich ako násilných kriminálnikov. Dezinformácie podkopávajúce protestné hnutie šírilo aj ďalších 936 účtov pravdepodobne z Číny. Podporovalo ich ďalších 200 000 automatických účtov. Všetky falošné účty boli zrušené. Spoločnosť pokračuje vo vyšetrovaní prípadu a nevylučuje, že budú odhalené ďalšie falošné účty.

Zamestnanci pripojili ukrajinskú jadrovú elektráreň na internet, kvôli ťažbe kryptomeny.

Ukrajinská tajná služba vyšetrovala incident, keď zamestnanci pripojili časť vnútornej siete jadrovej elektrárne na internet, aby mohli ťažiť kryptomeny. Vyšetrovanie sa zameralo tiež na preskúmanie možností útočníkov využiť ťažobné zariadenia na prienik do

systémov elektrárne a exfiltráciu citlivých dokumentov a informácií. Vyšetrovatelia zhabali dve zariadenia obsahujúce 5 a 6 kusov grafických kariet Radeon RX 470 v administratívnej časti komplexu. Ďalšie zariadenia zhabali v kasárňach národnej gardy, ktorá komplex stráži.

Francúzska polícia v spolupráci s firmou Avast rozbila botnet RETADUP a dezinfikovala vyše 850 000 zariadení.

Vyše 850 000 zariadení infikovaných botnetovým malvérom RETADUP na diaľku dezinfikovala francúzska polícia v spolupráci s výskumníkmi firmy Avast. Po odpojení C&C servera ho nahradila serverom, ktorý vysiela botom príkaz na sebazničenie. Server bude online ešte niekoľko mesiacov, aby mali možnosť aj ďalšie zariadenia zapojené do botnetu pripojiť sa a prijať príkaz. Francúzska polícia objavila ďalší kontrolný server v USA a kontaktovala FBI, na čo bol server odpojený. Botnet používali útočníci na ťažbu kryptomien, no mal tiež schopnosti vykonávať DDoS útoky a exfiltrovať citlivé dáta obetí.

Svetové módne a motoristické značky pod útokom Magecart – zasiahnutých 80 e-shopov.

Nechválne známe skupiny Magecart kompromitovali skriptom na krádež údajov z platobných kariet ďalších 80 internetových obchodov významných svetových módnych a motoristických značiek. Väčšina zo zasiahnutých webstránok fungovala na zastaraných zraniteľných verziách CMS Magento. Výskumníci spoločností Aite Group a Arxan Technologies nemenovali konkrétne spoločnosti, ktoré sa stali cieľom útoky, nakoľko sa jednalo o aktívnu kampaň. Útočníci mali vo svojom pláne zapojené nič netušiace osoby hľadajúce prácu online, ktorých úlohou bolo preposielať tovar, ktorý útočníci nakúpili ukradnutými kreditnými kartami, kupcom z východnej Európy.

Ruské autority zatkli útočníkov zo skupiny TipTop za šírenie bankových trójskych koní.

Ruské autority zatkli útočníkov zo skupiny TipTop, ktorí od roku 2015 nainfikovali 800 000 zariadení Android bankovými trójskymi koňmi. Kriminálnici si tak denne zarobili 1500 až 10 500 USD. Pri väčšine svojich kampaní používali trójskeho koňa Hqwar (Agent.BID), ktorý okrem svojej hlavnej činnosti – krádeže bankových prihlasovacích údajov – dokáže čítať SMS, nahrávať hovory a inicializovať USSD požiadavky. Skupina TipTop hrala významnú úlohu pri distribúcii malvéru ukrytého do aplikácií pre Android.

- **Údaje vyše milióna juhokórejských platobných kariet na predaj.**
- **Prienik na servery internetového obchodu s oblečením Poshmark. Unikli údaje miliónov klientov.**
- **Nezabezpečenú MongoDB databázu 2,1 milióna zákazníkov mexického kníhkupectva Librería Porrúa zamenili útočníci za odkaz s požiadavkou o výkupné.**
- **Desiatky počítačov vo Venezuele napadnutých malvérom, vrátane armádnych. Skupina Machete kradla da mesiace citlivé súbory.**
- **Prienik do systémov online obchodu StockX. Spoločnosť poslala svojim zákazníkom požiadavku na zmenu hesla.**
- **APT 28 používa zraniteľnosti populárnych IoT zariadení pre získanie prístupu do korporátnych sietí, informovalo Microsoft Threat Intelligence Center.**
- **Prienik do systémov CafePress spôsobil únik osobných údajov 23 miliónov zákazníkov tohto internetového obchodu.**
- **Nárast množstva „romantických podvodov“ na online zoznamkách. Kriminálnici tentokrát nepýtajú peniaze, ale žiadajú obete o prijímanie a presmerovávanie prevodov v rámci operácií spojených s praním špinavých peňazí.**
- **Zamestnanci AT&T dostali milión USD za nainštalovanie malvéru do zariadení firmy. Cieľom bolo získavanie informácií a získanie prístupu k zariadeniam. Akcia trvala 5 rokov.**
- **Masívna kampaň imitujúca webstránky Walmartu, MacDonaldu a iných spoločností zbiera osobné údaje obetí.**

TLP: White

- **Nezabezpečené Amazon S3 úložiská poskytovali prístup k medicínskym dátam 14 000 pacientov a 6 miliónom e-mailových adries Democratic Senatorial Campaign Committee.**

- **Útočník požadoval od kryptomenovej burzy Binance výkupné 300 BTC (asi 3,5 milióna USD) za to, že nezverejní citlivé osobné údaje a dokumenty 10 000 zákazníkov.**

- **Americká banková a poisťovacia spoločnosť State Farm zachytila útok typu credential stuffing (skúšanie prihlasovacích údajov uniknutých z iných databáz), pričom sa útočníci úspešne prihlásili do nešpecifikovaného množstva účtov.**

- **Magecart útok na newyorkskú National Baseball Hall of Fame. Útočníci pol roka kradli platobné údaje.**

- **Nezabezpečená MongoDB databáza španielskej eskortnej služby poskytovala prístup k citlivým údajom o dievčatách, financiách spoločnosti aj zákazníckym hodnoteniam.**

- **Pikantná zoznamka 3Fun mala horšie bezpečnostné diery ako Grindr a Romeo. Ohrozila tak súkromie asi 1,5 milióna používateľov.**

- **Úspešný phishingový útok na aerolinky Air New Zealand ohrozil dáta zákazníkov prihlásených v Airpoints loyalty programe.**

- **Vyše 33 aplikácií pre Android dostupných cez Google Play obsahovalo trójskeho koňa. Spolu mali vyše 100 miliónov stiahnutí.**

- **Prienik do slabo zabezpečenej databázy Biostar 2 spoločnosti Suprema znamenal únik 28 miliónov citlivých záznamov, vrátane vyše milióna biometrických údajov.**

- **Facebook sledoval a prepisoval audio-komunikáciu používateľov na Messengeri, aby testoval spoľahlivosť algoritmov umelej inteligencie.**

- **Databáza 321 000 používateľov hackerského fóra Cracked.to skončila na konkurenčnom fóre RaidForums – podobne ako v máji OGusers.**

- **Unikla nezabezpečená MongoDB databáza hotelovej spoločnosti Choice Hotels. Obsahovala 700 000 citlivých záznamov zákazníkov, za ktoré útočníci žiadajú výkupné.**

- **Útočníci prenikli do platobných systémov 250 pobočiek reťazca Hy-Vee. Spoločnosť varuje zákazníkov, ktorí u nej platili v poslednom čase kartou.**

- **Prienik do systémov, či nezabezpečená databáza umožnili prístup k citlivým**

údajom a vizuálnemu materiálu z vyše milióna účtov stránky pre dospelých Luscious.

- Magecart skript na krádež údajov z kreditných kariet nájdený na stránke PokerTracker.com.
- Podvodníci ukradli citlivé osobné údaje americkým veteránom a pripravili ich následne o milióny dolárov.
- Bezpečnostný výskumník našiel aktívne rastúcu nezabezpečenú databázu s 161 miliónmi nešifrovaných záznamov. Patrila spoločnosti MoviePass. Dostupné boli aj platobné karty 58 000 zákazníkov.
- 80 podvodníkov, najmä Nigérijcov, zapojených do BEC podvodov (Business Email Compromise) a zoznamkových podvodov pred súdom za krádež 6 miliónov USD a pokus o krádež ďalších 40 miliónov USD.
- Únik citlivých dát klientov vernostného programu Mastercard Priceless Specials. Údaje zverejnili útočníci na internete.
- Prienik do systémov jedného z najväčších poskytovateľov webhostingových služieb Hostinger. Exponované boli osobné informácie 14 miliónov klientov.
- Spear-phishingové útoky na kritickú infraštruktúru na strednom východe. Skupina LYCEUM využíva nový malvér.
- Bezpečnostná spoločnosť Imperva utrpela prienik. Unikli dáta časti klientov využívajúcich Cloud Web Application Firewall, tiež známy ako Incapsula.
- Bezpečnostní výskumníci spoločnosti Kaspersky objavili malvér v aplikácii CamScanner pre zariadenia Android. Google ju odstránil zo svojho Play Store.
- Výskumníci z Cisco tímu Talos zachytili niekoľko aktívnych kampaní na svetové vládne a finančné inštitúcie. Útočníci vytvárajú zadné vrátka malvérmi Orcus a Revenge.
- USA spustila kybernetický útok na databázu, ktorú používal Irán pri plánovaní útokov na tankery v Perzskom zálive.
- Útočníci kompromitovali poskytovateľa softvéru pre zubné ambulancie a infikovali stovky zubárskych praxí v USA.
- Austrálska sieť reštaurácií TGI Fridays odporučila zákazníkom svojho vernostného programu zmeniť heslá po tom, ako nechala citlivú databázu otvorenú na internete.

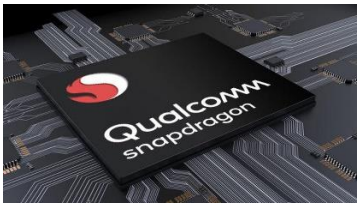
TLP: White

- **Niekoľko desiatok ruských hardvérových zariadení pre odpočúvanie internetovej komunikácie bolo prístupných z internetu, pričom mohli unikať citlivé dáta.**

- **Prienik do webových používateľských účtov spoločnosti Foxit. Unikli dáta z účtov a spoločnosť vynucuje zmenu hesiel.**

Závažné zraniteľnosti bežných softvérových produktov

QualPwn - Ako ovládnuť Android zariadenie pomocou zraniteľností čipov Qualcomm



Bezpečnostný tím Blade spoločnosti Tencent našiel tri zraniteľnosti súhrnne označené ako QualPwn, nachádzajúce sa v čipoch Qualcomm, využívaných v zariadeniach Android. Útočníkom s prístupom na WLAN, ku ktorej je pripojené zraniteľné zariadenie, umožňujú na tomto zariadení vykonávať kód a prevziať nad ním kontrolu. Útok si nevyžaduje interakciu používateľa.

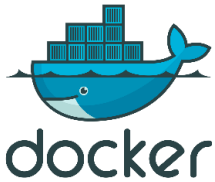
Desiatky ovládačov pre Windows umožňujú ovládnuť systém

Výskumníci spoločnosti Eclypsium študovali vyše 40 ovládačov od 20 spoločností. Objavili v nich zraniteľnosti vedúce ku zvýšeniu práv a k možnosti čítať a zapisovať do systémovej pamäte a registrov. Takto môžu útočníci vykonávať kód so systémovými právami, či zasahovať do firmvéru. Na zraniteľnom zariadení dokážu získať perzistenciu a kompletne ho ovládnuť.

Chyba Auth0 Passport-SharePoint umožňuje obísť autentifikáciu

Kvôli neprítomnosti overovania JWT podpisu prístupového tokenu môže útočník v produkte Passport-SharePoint falšovať tokeny a tým obísť autentifikáciu.

Chyba v platforme Docker



Platforma pre vývoj, dodanie a beh aplikácií Docker, konkrétne jej súčasť docker-credential-helpers obsahuje zraniteľnosť, ktorá môže viesť k vytvoreniu DoS podmienok pomocou chyby dvojitého uvoľnenia miesta v pamäti.

TLP: White

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Enterprise NFV Infrastructure Software (CVE-2019-1895): zraniteľnosť umožňuje obísť autentifikáciu kvôli nedostatočnej autentifikácii pri vytváraní VNC relácie.
Cisco Enterprise NFV Infrastructure Software (CVE-2019-1946): nevhodná autentifikácia pri prístupe do webového manažovacieho rozhrania umožňuje útočníkom obchádzať autentifikáciu.
Cisco Firepower Management Center (CVE-2019-1949): kvôli nevhodnej sanitizácii používateľského vstupu môže útočník vykonávať HTML kód a skripty v kontexte zraniteľného prehliadača.
Cisco IOS XE Software: kvôli nevhodnej kontrole v kóde manažujúcom Cisco REST API autentifikáciu môže útočník získať identifikátor tokenu prihláseného používateľa a obísť autentifikáciu.
Cisco Firepower Threat Defence Software (CVE-2019-1981): v normalizačnej funkcionalite existuje zraniteľnosť, ktorá umožňuje vzdialené obídenie zabezpečenia a vykonanie nepovolených úkonov.
Cisco Integrated Management Controller (CVE-2019-1850, CVE-2019-1863, CVE-2019-1871, CVE-2019-1885, CVE-2019-1896, CVE-2019-1908): Produkt Cisco Integrated Management Controller obsahuje niekoľko závažných zraniteľností. Kvôli nevhodnej kontrole používateľského vstupu je možné do webového rozhrania zariadenia, CSR a CLI (špecificky Redfish protokol) injektovať príkazy s právami používateľa root. Taktiež je možné obísť autentifikáciu. Ďalšia zraniteľnosť súvisí s pretečením medzipamäte v nástroji Import Cisco IMC a umožňuje útočníkom vykonávať ľubovoľný kód s právami používateľa root. Implementácia rozhrania IPMI obsahuje zraniteľnosť umožňujúcu únik citlivých informácií.
Cisco – viaceré produkty (CVE-2019-1937): nedostatočné vyhodnocovanie hlavičiek požiadaviek vedie k obídeniu autentifikácie a získaniu administrátorského prístupu ku zraniteľnému zariadeniu.
Cisco HyperFlex (CVE-2019-12621): nedostatky v narábaní s kryptografickými kľúčmi vedú k možnosti získať šifrovací kľúč klastra. Útočník následne môže vykonávať man-in-the-middle útoky.

Zraniteľnosti VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
CVE-2019-11477, CVE-2019-11478: chyby súvisiace s implementáciou SACK v linuxovom jadre.

TLP: White

CVE-2019-5521: zraniteľnosť typu čítanie mimo povolených hraníc, ktorá môže viesť k úniku informácií.

Zraniteľnosť ovládača displeja NVIDIA

Ovládač displeja NVIDIA GPU obsahuje kritickú zraniteľnosť, ktorá umožňuje navýšenie práv a vykonávanie ľubovoľného kódu. Tá sa nachádza konkrétne v komponente DirectX. Útočník ju môže zneužiť pomocou špeciálne vytvoreného shadera, ktorý spôsobí prístup mimo povolené hranice v lokálnom dočasnom poli shadera.

Zraniteľnosť Intel RAID Web Console

V aplikácii Intel RAID Web Console môže útočník obísť autentifikáciu a získať prístup k citlivým informáciám. Tieto môže zneužiť pre ďalšie útoky.

Zraniteľnosť Microsoft Azure

V produkte Microsoft Azure Active Directory môže útočník vzdialene dosiahnuť zvýšenie práv kvôli chybe knižnice Azure Active Directory Authentication Library pri narábaní s tokenom.

Kritická zraniteľnosť Linuxového jadra

V jadre operačného systému Linux verzií starších ako 4.11 sa nachádza kritická zraniteľnosť CVE-2017-18509. Útočníkom umožňuje vykonávať ľubovoľný kód v kontexte danej aplikácie kvôli chybe pri overovaní 'sk_type' a protokolu v súbore 'net/ipv6/ip6mr.c'.

Kritická zraniteľnosť v Palo Alto Networks PAN-OS

Kritická zraniteľnosť CVE-2019-1582 v systéme PAN-OS umožňuje spôsobiť nešpecifikované vzdialené poškodenie pamäte. Útočník tak môže vykonávať ľubovoľný kód s právami používateľa, ktorý spustil danú aplikáciu. Zraniteľné sú systémy PAN-OS vezrií 8.1.9 a starších, a tiež 9.0.3 a starších.

Mesačník zraniteľností August 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
    - Ovládače pre Windows
    - Čipy Qualcomm

https://www.csirt.gov.sk/aktualne-7d7.html?id=200