ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Október 2018

Vypracoval: CSIRT.SK

TLP: White

Podľa prieskumu spoločnosti Gemalto v prvej polovici roka 2018 uniklo v svetovom merítku 4,5 miliardy záznamov, čo predstavuje 173% uniknutých dát v roku 2017 a 1800% uniknutých dát z roku 2015. Priemerne za sekundu teda uniklo 291 záznamov. Zodpovední boli ako útočníci, tak aj niektoré spoločnosti, ktoré nesprávne nakonfigurovali zabezpečenie svojich databáz. Takto získané osobné údaje môžu byť zneužité napríklad na spear phishing, teda cielenú formu phishingu. Útočník, ktorý o vás získal zopár správnych základných údajov, dokáže odvodiť vašu pracovnú pozíciu, koníčky a ďalšie charakteristiky, podľa ktorých dokáže sformulovať presvedčivý podvodný e-mail. V ňom môže poslať škodlivú prílohu, alebo odkaz, či v mene dôveryhodnej organizácie, alebo osoby vás požiadať o prihlasovacie údaje, platobné údaje, alebo platbu na svoj účet. Kam až môže zájsť spear-phishing môžete vidieť nižšie v popise kampane FASTCash, počas ktorej z bánk cez bankomaty ukradli útočníci milióny dolárov. Podarilo sa im to vďaka nedostatočne zaškoleným zamestnancom inštitúcií, ktorých primäli otvoriť škodlivé prílohy.

Krádeže osobných údajov podľa prieskumu spoločnosti Blueliv stúpli medzi júnom a augustom 2018 voči obdobiu marec-máj v severnej Amerike o 141%, zatiaľ čo v Európe a Ázii bol zaznamenaný mierny pokles o 22% a 36%. Minimálna cena za osobné údaje jednej obete sa na darknete v rovnakom období pohybovala medzi 2 až 100 dolármi.

Phishing je podľa spoločnosti IDG stále najbežnejším vektorom útokov na organizácie. Prieskum spoločnosti MediaPRO, ktorého časť bola zameraná aj na testovanie obozretnosti zamestnancov voči phishingu, hovorí, že v USA majú nedostatočné bezpečnostné povedomie 3 zo 4 zamestnancov. Títo nechcene ohrozujú bezpečnosť spoločností, pre ktoré pracujú. Na phishing reagovalo správne 86% nižšie postavených zamestnancov, a iba 69% manažmentu. V rámci sektorov dopadli najhoršie zamestnanci finančných inštitúcií. Takmer 20% z nich pokladalo otvorenie prílohy phishingovej správy za vhodnú reakciu. Takto je možné jediným kliknutím kompromitovať dáta celej organizácie, ako sa môžeme presvedčiť napríklad vo video-ukážke tu.

Neustále preškoľovanie personálu je potrebné nielen kvôli ľudskej zábudlivosti, ale aj preto, že útočníci svoje metódy stále zlepšujú a diverzifikujú. Jednou z možností, ako zvýšiť dôveryhodnosť phishingovej domény, je získať platný certifikát. Nižšie popisujeme konkrétny príklad, kedy na to útočníci využili službu Azure Blob. Podobne bola zneužitá služba zdieľania súborov cez webový prehliadač Cloudflare IPFS. Vylepšujú sa aj útočníci využívajúci vishing, teda „voice phishing“. Jedná sa o telefonáty, často aspoň čiastočne automatizované, pri ktorých sa útočník snaží vzbudiť dojem, že obeti volá dôveryhodná inštitúcia, u ktorej má založený účet, alebo je s ňou v inej forme interakcie.

Bezpečnostní výskumníci si uvedomujú pokrok zločincov a pripravujú sa na nové hrozby. Pozorovaním a imitovaním aktuálnych phishingových hrozieb spoločnosť Cyxtera simuluje možné zneužitie open source umelej inteligencie na šírenie phishingu v programe DeepPhish.

Na koľko si ceníte svoje osobné údaje vy? Študenti z Brown University v Providence, USA ich radi vymenia za šálku kávy.

Riešené incidenty na Slovensku a z našej činnosti

V mesiaci október sa odohral jeden významný útok na infraštruktúru SR, ktorý bol aj medializovaný. Jednalo sa o útok na Ministerstvo zahraničných vecí SR.

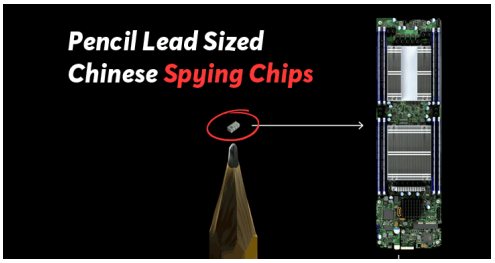
V mesiaci október riešil CSIRT.SK štandardne prevažne phishingové kampane na svoju konštituenciu. Okrem toho riešil brute force útok na e-mailové účty pracovníkov jednej organizácie.

V rámci svojej proaktívnej činnosti CSIRT.SK simuloval DoS útok na jednu organizáciu, aby preveril odolnosť jej systémov. Taktiež vykonával penetračných testy v rámci svojej konštituencie. V mesiaci október vykonal CSIRT.SK pravidelný test protokolov SSL/TLS na webstránkach svojej konštituencie. O výsledkoch boli organizácie so zraniteľnými webstránkami informované.

V rámci edukatívnej činnosti viedol CSIRT.SK dvojdňový seminár na tému informačnej bezpečnosti pre ÚPVII. V rámci prednášok urobili školitelia reálne ukážky, akými spôsobmi je možné získať informácie a kompromitovať zariadenie obete. Tiež urobili interaktívny phishingový test, kde poukázali na hlavné znaky phishingových e-mailov. Ako výstup zo školenia publikoval CSIRT.SK na svojom webe video ukážku, ako funguje napadnutie malvérom typu RAT (Remote Access Tool) - Remcos.

Významné útoky vo svete

Čína infiltrovala americké spoločnosti pomocou miniatúrneho čipu



Začiatkom októbra sa na spravodajskej stránke spoločnosti Bloomberg objavila správa, že na matičných doskách pre servery od spoločnosti Super Micro boli objavené mikročipy o veľkosti zrnka ryže. Tieto mali byť na dosky umiestnené počas výrobného procesu v čínskych továrňach a mali poskytovať možnosť otvoriť komunikáciu, posielať príkazy a exfiltrovať citlivé informácie. Servery Super Micro využívajú veľké americké spoločnosti ako Apple, či Amazon, no aj vládne inštitúcie. Nedlho po zverejnení článku sa dostavili reakcie amerických a čínskych vládnych inštitúcií, ako aj Apple, Amazon a Super Micro, ktoré túto správu dôrazne dementovali a predstavili niekoľko silných argumentov, prečo k podobnej situácii nemohlo dôjsť.

Vyše 100 000 routerov presmerovaných s cieľom krádeže bankových údajov

Čínski bezpečnostní výskumníci odhalili malvérovú kampaň, ktorá v niekoľkých krokoch kradla prístupové údaje obetí k internet bankingu. Nazvali ju GhostDNS, pretože malvér v prvom kroku ovládol domáci router obete, následne na ňom zmenil nastavenia DNS serverov a nakoniec poslal obeť na škodlivú phishingovú verziu bankovej webstránky. Kampaň sa zameriavala na routery chránené slabým heslom, prípadne bez hesla, s administrátorským rozhraním dostupným cez internet. Zasiahnutých bolo vyše 100 000 routerov, pričom takmer 88% pochádzalo z Brazílie.

5 zo 6 routerov nie je aktualizovaných

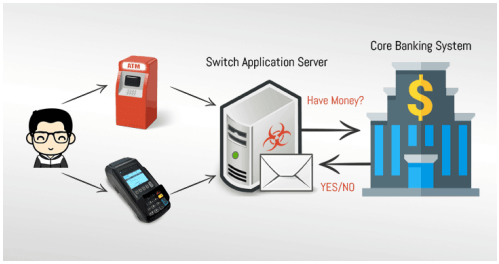
Štúdia amerických spotrebiteľov skúmajúca vzorku 186 domácich wifi routerov 14 výrobcov ukázala, že 5 zo 6 domácich routerov nie je aktualizovaných a obsahuje zneužiteľné zraniteľnosti. Táto malá vzorka vykazovala neuveriteľných 32 003 zraniteľností v 155 zariadeniach, čo predstavuje priemerne 186 zraniteľností na jeden zraniteľný router. Z nich vyše štvrtina spadala pod kritické, alebo závažné.
Pre zaujímavosť, medzičasom sa našiel rusky hovoriaci

gray-hat hacker Alexey, ktorý odstránil malvér, aktualizoval a ošetril bezpečnostné nastavenia už na vyše 100 000 MikroTik routeroch.

Sieť reštaurácií v Kanade uzavrená kvôli infekcii malvérom

Niekoľko značiek kanadskej reštauračnej siete Recipe Unlimited zaznamenalo po celej krajine víkendový výpadok svojich IT systémov po tom, ako spoločnosť tieto systémy odpojila ako reakciu na šírenie ransomvéru, pravdepodobne Ryuk. V dobe, keď boli prevádzky odpojené, nemohli spracovávať platby kartou. Niektoré prevádzky sa rozhodli dočasne zatvoriť. Súhrnne sa hovorilo až o 1400 pobočkách.

Bankové servery hacknuté, bankomaty vydávajú hotovosť



Skupina označovaná ako APT Hidden Cobra, spájaná so severokórejským režimom, odcudzila milióny dolárov výbermi z bankomatov. V kampani FASTCash napadla malvérom switch application servery bánk, v ktorých mali jej členovia účty s minimálnym, či nulovým zostatkom. Tieto servery slúžia na komunikáciu so systémami bánk, a teda aj na overenie zostatku klienta. Malvér toto overenie dokázal obísť a poslať bankomatu falošné odsúhlasenie transakcie. Útočníci infikovali servery pomocou spear-phishingovej kampane, v ktorej zamestnanci bánk dostali e-maily so škodlivou prílohou.

Instagram ako trhovisko - kradnuté účty v online hre Fortnite, či prenájom botnetu

Veľký záujem o hru Fortnite podnecuje ziskuchtivých útočníkov ku kompromitácii užívateľských účtov, cez ktoré následne môžu kupovať herné vylepšenia a prevádzať ich na svoje účty. Okrem toho sa na Instagrame objavujú inzeráty na prenájom botnetov, ako napríklad Mirai. Ceny sa môžu pohybovať okolo 5 až 80 dolárov za mesiac. Pre zabezpečenie herných (a iných) účtov sa odporúča používať odlišné heslá, nenechať sa oklamať podvodnými telefonátmi, či e-mailami požadujúcimi oznámenie hesla, či využívať dvojfaktorovú autentifikáciu.

Phishingové kampane využívajú Azure Blob Storage na zvýšenie dôveryhodnosti

Úroveň poznatkov bežných užívateľov ohľadne IT bezpečnosti sa stále zvyšuje. Mnohí užívatelia dokážu odhaliť phishingovú stránku na základe certifikátu, ktorý nepatrí spoločnosti, ktorú sa stránka snaží imitovať. Útočníci tak prišli s jednoduchým riešením. Na odcudzenie osobných údajov pre služby spoločnosti Microsoft začali využívať službu Microsoft Azure, resp. Azure Blob Storage, kde umiestnia svoj formulár. Keď obeť tento dokument otvorí, vidí stránku podpísanú certifikátom Microsoft, čo u nej vzbudí dôveru, aby zadala svoje prihlasovacie údaje, napríklad do MS Office 365 (takýto útok bol reálne pozorovaný).

Sony smart TV zraniteľné voči vzdialenému prístupu

Bezpečnostní výskumníci objavili niekoľko zraniteľností v ôsmich modeloch televízorov Sony Bravia, z ktorých jedna je kritická. Umožňuje útočníkom spúšťať na zariadení ľubovoľné príkazy, čo môže viesť až k možnosti vzdialene vykonávať kód s administrátorskými privilégiami. Útočníkom sa tak môže otvoriť cesta k ďalším zariadeniam na rovnakej lokálnej sieti, či možnosť zneužiť zariadenie v botnete. Vďaka výkonnému grafickému procesoru je možné na smart TV tiež ťažiť kryptomeny. Vlastníkom TV dnes teda nezostáva iná možnosť, ako sledovať a inštalovať do svojich zariadení softvérové aktualizácie.

Krádeže WhatsApp účtov cez hlasovú službu

Nový útok na online účty potrebuje len vaše telefónne číslo. Útočník môže bez interakcie používateľa presunúť jeho telefónne číslo do svojho WhatsApp účtu. Stačí, ak zašle požiadavku na registráciu čísla obete. WhatsApp zašle na číslo obete overovací kód, ktorý útočník nevidí, no môže požiadať o hlasovú správu. Užívatelia štandardne ponechávajú prednastavený pin na prístup do hlasovej schránky, ktorý sa dá nájsť na internete. Útočník tak ľahko získa potrebný overovací údaj a následne môže nastaviť dvojfaktorovú autentifikáciu, čím obeť vymkne z jej WhatsApp účtu. Výskumník, ktorý na tento útok upozornil, spomenul, že potenciálne zraniteľné sú aj ďalšie služby, ako PayPal, Netflix, Instagram, LinkedIn, Apple, Google, Microsoft a Yahoo.

Možný únik údajov z 500 000 účtov, Google+ odstavené

Sociálnu sieť Google+ čaká ukončenie činnosti. Dopomohlo k tomu objavenie chyby v API služby, ktorá umožňovala exfiltrovať osobné údaje 500 000 používateľov aj v prípade, že ich niektorí používatelia nezdieľali. Spoločnosť Google sa vyjadrila, že neexistujú dôkazy o takejto exfiltrácii, napriek tomu, že chyba existovala v aplikácii 3 roky. K službe však pristupovali stovky aplikácií, ktoré potenciálne mohli získavať tieto informácie. Vyhlásila tiež, že vzhľadom na nízku používanosť služby sa neoplatí ďalej venovať úsilie na jej udržiavanie a zabezpečovanie a službu nebude naďalej od začiatku roka 2019 prevádzkovať. Namiesto toho ju konvertuje na komerčný produkt pre firmy.

Stratený USB kľúč – únik dát letiska Heathrow

Kuriózny bezpečnostný incident sa stal v Londýne, kde okoloidúci našiel na zemi ležať USB kľúč, obsahujúci veľké množstvo súborov s dátami o bezpečnostných systémoch a opatreniach na letisku Heathrow. Nálezca informoval týždenník The Sunday Mirror, ktorý incident rozobral v článku. Dáta okrem iného obsahovali citlivé osobné údaje vysokopostavených bezpečnostných pracovníkov, bezpečnostné trasy pre politických činiteľov a kráľovnú a časové rozvrhy hliadok. Spoločnosť zodpovedná za bezpečnosť letiska dostala za nedbalosť pokutu.

Spoločnosti Garmin Navionics unikli dáta stotisícok zákazníkov

Jedná sa o ďalší prípad nezabezpečenej MongoDB databázy. Spoločnosť Navionics vo vlastníctve Garmin vlastnila bezpečnostne nevhodne nakonfigurovanú databázu s údajmi vyše 261 000 zákazníkov, ktoré obsahovali e-mailové adresy, mená, identifikačné čísla zakúpených produktov a užívateľov a softvérové údaje, ako navigačné dáta lodí.

Vyše 9 miliónov kamier a DVR zariadení zraniteľných a ľahko ovládnuteľných útočníkmi

Bezpečnostní výskumníci zo spoločnosti SEC Consult oznámili, že milióny zariadení sú jednoducho napadnuteľné a zneužiteľné na špionáž, či zapojenie do botnetu. Jedná sa o zariadenia od vyše 100 značiek, ktoré odoberajú výrobky od čínskej spoločnosti Hangzhou Xiongmai Technology Co., Ltd. Hlavným problémom je nedostatočné zabezpečenie prístupu k užívateľským účtom zariadení na cloude.

Falošné aktualizácie Adobe Flash Player inštalovali malvér ťažiaci kryptomeny

Aj techniky na šírenie malvéru na ťaženie kryptomien sa vylepšujú. Výskumník Brad Duncan z Palo Alto Unit 42 informoval o kampani šíriacej trójskeho koňa, ktorý sa tvári ako aktualizácia aplikácie Flash Player. Ako novinku okrem inštalácie malvéru ťažiaceho kryptomenu Monero skutočne nainštaluje aj spomínanú aktualizáciu. Vďaka tomu zníži šancu, že obeť nadobudne podozrenie, že niečo nie je v poriadku. Pri inštalácii aktualizácií dbajte na to, aby zdroj inštalačného súboru boli vždy legitímne stránky spoločnosti, ktorá daný produkt vyvíja.

Prienik do systémov webhostingovej spoločnosti Hetzner South Africa

Útočníkom sa zneužitím zraniteľnosti typu SQL injection tento mesiac podarilo preniknúť do systémov webhostingovej spoločnosti Hetzner South Africa. Jedná sa o druhý úspešný útok na spoločnosť za obdobie posledného roka. Odcudzili osobné údaje približne 40 000 zákazníkov v rozsahu mien, e-mailových adries, telefónnych čísiel, adries, identifikačných čísiel, DIČ a čísiel bankových účtov. Citlivé platobné údaje údajne neunikli. Spoločnosť varovala pred možnosťou zneužitia uniknutých údajov v personalizovaných phishingových kampaniach.

Údaje desiatok miliónov zákazníkov FitMetrics voľne dostupné na internete

Skupina serverov ElasticSearch bola vystavená na internete bez ochrany heslom. Útočníkovi teda stačilo zistiť IP adresu servera a mohol sa okrem iného dostať aj k osobným údajom používateľov FitMetrics a informáciám o zariadeniach a dátových bodoch. Údaje používateľov obsahovali napríklad meno, dátum narodenia, e-mailové adresy, telesné miery a indikátory pre FitMetrix softvér. Zasiahnuté mohli byť milióny používateľov, aj keď presné čísla nie sú známe. Výskumníci zistili, že na serveroch bol už umiestnený odkaz so žiadosťou o výkupné, aby neznámy útočník nezverejnil exfiltrované dáta. Spoločnosť FitMetrics, ktorá poskytuje softvér na monitoring srdcového tepu pre športové a medicínske aplikácie, bola tento rok odkúpená spoločnosťou Mindbody.

Unikli údaje o kreditných kartách 30 000 zamestnancov Ministerstva obrany USA

Začiatkom októbra bol odhalený únik cestovných záznamov približne 30 000 vojenských aj civilných zamestnancov Pentagonu. Dáta boli spravované externým dodávateľom služby a pozostávali z osobných údajov zamestnancov a údajov o ich platobných kartách.

Údaje 35 miliónov voličov z USA na predaj

Na Dark Webe sa dali kúpiť záznamy 35 miliónov amerických voličov z 19 štátov. Údaje obsahovali dostatok informácií na identifikovanie voličov a ich volebnej histórie – mená, adresy a telefónne čísla, a pod.. Majiteľ týchto údajov by mohol spáchať hromadnú krádež identity a prekaziť volebný proces. Na predaj boli databázy z jednotlivých štátov v cenovom rozsahu 150-12 500$, podľa množstva záznamov. Po zakúpení databáz sľuboval predajca ich bezplatné sprístupnenie pre všetkých registrovaných užívateľov predmetného fóra. Tento systém podporoval možnosť kúpy s využitím hromadnej zbierky medzi používateľmi.

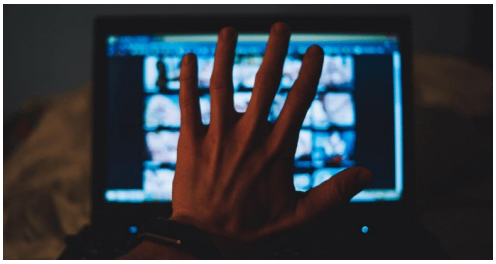
Nový malvér útočí na kritickú infraštruktúru

Malvér s názvom GreyEnergy, podobný BlackEnergy, ohrozuje kritickú infraštruktúru a priemyselné systémy SCADA. Malvér zatiaľ vykazuje výzvednú aktivitu, ako vytváranie zadných dvierok, krádež súborov, zaznamenávanie stlačených kláves a odosielanie screenshotov. Vzhľadom na jeho modulárnu architektúru však do neho môžu byť časom zabudované aj deštrukčné prvky.
Štúdia spoločnosti CyberX hovorí, že priemysel vrátane kritickej infraštruktúry ostáva pomerne ľahko zraniteľný. Problémom je nedôsledný prístup k odstraňovaniu známych zraniteľností, používanie zastaraných a nepodporovaných systémov ako Windows XP či Windows Server 2003 a dostupnosť zvonku. Podľa prieskumu až 40% spoločností má systémy pripojené na internet a až 84% študovaných organizácií malo aspoň jedno zariadenie prístupné zvonku s otvorenou komunikáciou cez RDP, SSH, VNC a podobne.

Prienik do systémov Healthcare.gov postihol 75 000 používateľov

Systém Federally Facilitated Exchanges, slúžiaci na registrovanie nových poistencov do zdravotného poistenia Obamacare (oficiálny portál je HealthCare.gov), bol napadnutý a došlo k úniku osobných údajov 75 000 registrovaných používateľov. Incident bol postúpený FBI.

Z databázy stránky pre dospelých unikli údaje 1,2 milióna používateľov



Databáza webstránky Wife Lovers, ktorú využívalo ďalších 7 stránok, obsahovala 1,2 milióna unikátnych e-mailových adries. Ďalšie užívateľské dáta, ktoré unikli, boli šifrované heslá, identifikátory príspevkov a IP adresy použité pri registrácii. Databáza bola šifrovaná 40 rokov starou hašovacou funkciou DEScrypt, ktorú je možné pomerne jednoducho prelomiť.

Únik dát ďalšej leteckej spoločnosti

V posledných mesiacoch došlo k niekoľkým veľkým únikom dát leteckých spoločností. Tento raz prišla na rad spoločnosť Cathay Pacific. Incident bol zaznamenaný ešte v prvej štvrtine roka a postihol 9,4 milióna zákazníkov. Spoločnosti unikli mená pasažierov, národnosti, dátumy narodenia, telefónne čísla, adresy, e-mailové kontakty, čísla pasov a občianskych preukazov a informácie o letoch. Vyše 400 zákazníkom unikli aj platobné údaje ku kreditným kartám.

Unikla databáza prispievateľov americkej strany Demokratov

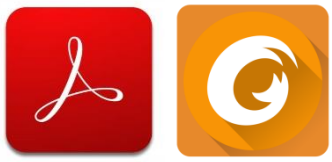
Konzultačnej firme zastrešujúcej prispievateľov pre americkú Demokratickú stranu unikla databáza prispievateľov, a tiež heslá k databázam voličov. Dáta boli uložené na nezabezpečenom sieťovom úložisku (NAS). Okrem iného obsahovali mená, adresy, telefónne a e-mailové kontakty, zmluvy a poznámky. Výskumníci zistili, že k zariadeniu bolo pristupované z viacerých IP adries z rôznych krajín.

Ďalšie obete minulo-mesačného úniku dát British Airways

Septembrový únik údajov leteckej spoločnosti British Airways, spojený s útokom pomocou malvéru MageCart, má 77 000 nových obetí. Spoločnosť to zistila pri prešetrovaní incidentu. Vo svojom vyhlásení uviedla, že týmto dodatočným obetiam mohli uniknúť kompletné platobné informácie ku kreditným kartám. K tomu mohlo uniknúť ďalších 108 000 sád platobných údajov bez CVV čísiel. Ako pozitívum však spoločnosť svoj minulomesačný odhad „prvej skupiny“ obetí znížila z 380 000 na 244 000.

Závažné zraniteľnosti bežných softvérových a hardvérových produktov

Kritické zraniteľnosti PDF prehliadačov Adobe a Foxit



Spoločnosť Foxit Software vydala opravu 124 rôznych zraniteľností v produktoch Foxit Reader a Foxit PhantomPDF pre Windows. Množstvo z nich je označených ako kritické. Spoločnosť Adobe tiež vydala opravu na 86 zraniteľností, z ktorých vyše polovica bola označená ako kritické. Zneužitie mnohých z nich môže viesť ku vzdialenému vykonávaniu kódu, alebo úniku informácií.

Pozor na chybnú aktualizáciu Windows 10 na verziu 1809

Chyba v októbrovej aktualizácii pre Microsoft Windows 10 na verziu 1809 spôsobuje mazanie používateľských súborov v zložke Documents. Okrem toho bol hlásený problém s kompatibilitou s ovládačom Intel Display Audio a zobrazovaní aktuálneho využitia procesora v utilite Task Manager. Microsoft zastavil distribúciu až do prešetrenia problému.

Zraniteľnosť MikroTik routerov je oveľa vážnejšia, ako sa predpokladalo

Zraniteľnosť MikroTik routerov, o ktorej sme písali v septembri, predstavuje oveľa väčší problém, ako sa predpokladalo. Útočníkom totiž okrem prístupu do routera, čítania súborov v jeho pamäti a odpočúvania komunikácie umožňuje aj obídenie firewallu routera, prístup k root shell a vzdialené vykonávanie kódu.

Microsoft opravil aktívne zneužívanú zraniteľnosť

Spoločnosť Microsoft vo svojom októbrovom balíku opráv okrem iného odstránila z operačného systému Windows aktívne zneužívanú zero-day zraniteľnosť, ktorá umožňuje útočníkom zvýšenie privilégií, vykonávanie kódu v režime jadra, manipuláciu s dátami a vytváranie nových účtov s právami používateľa.

Chyba v LibSSH dovoľuje autentifikáciu bez hesla

Kritická zraniteľnosť v LibSSH predstavuje pre útočníka možnosť prihlásiť sa na server bez zadania hesla. Postačuje oznámiť serveru, že prihlásenie prebehlo úspešne a kvôli chybe pri overovaní server správu príjme ako platnú. Táto chyba je v LibSSH prítomná už štyri roky, od verzie 0.6.

Kritické zraniteľnosti v produktoch Oracle

ORACLE®
WebCenter

Spoločnosť Oracle vydala v októbrovom balíku aktualizácií opravy 301 zraniteľností svojich produktov. Najvážnejšia zraniteľnosť s hodnotením 10/10 sa nachádza v produkte GoldenGate a útočník ju dokáže zneužiť jednoduchým spôsobom vzdialene a bez autentifikácie. Následne dokáže prevziať úplnú kontrolu nad aplikáciou a jej pridruženými systémami. Podobný spôsob zneužitia je možný u 45 kritických zraniteľností ďalších produktov Oracle.

Odhalená mnohoročná zero-day zraniteľnosť jQuery

jQuery
write less, do more.

Osem rokov stará závažná zraniteľnosť v module frameworku jQuery s názvom jQuery File Upload bola odhalená výskumníkom spoločnosti Akamai. Útočníkom umožňuje bez autentifikácie nahrať na server ľubovoľný kód a spúšťať vzdialene príkazy s privilégiami servera. Zraniteľnosť súvisí so zmenou v softvéri Apache HTTP Server, pričom súbor s bezpečnostnými nastaveniami .htaccess bol v prednastavenej konfigurácii zakázaný.

Zero-day zraniteľnosť vo Windows 10 umožňuje mazať systémové súbory

Závažná zero-day zraniteľnosť v systémoch Windows 10, Windows Server 2016 a Windows Server 2019 bola zverejnená na Twitterovom účte používateľa SandboxEscaper. Zraniteľnosť umožňuje zvýšiť privilégiá používateľa na úroveň administrátora a potenciálne nahradiť kritické systémové súbory upravenou škodlivou verziou.

Dve kritické zraniteľnosti CMS Drupal

Podporované verzie CMS Drupal obsahujú dve kritické zraniteľnosti umožňujúce vzdialené vykonávanie kódu. Okrem nich boli objavené tri stredne závažné zraniteľnosti týkajúce sa otvoreného presmerovania a obídenia prístupových práv. Všetky zraniteľnosti boli opravené v aktualizáciách podporovaných verzií 7.x, 8.5.x a 8.6.x spoločnosťou vyvíjajúcou toto CMS.

Tri kritické zraniteľnosti D-Link routerov - nie všetky modely budú opravené

Tri rôzne kritické zraniteľnosti boli objavené v niekoľkých modeloch D-Link routerov. Útočníkovi umožňujú vykonať traverzovanie cesty, získať prístupové administrátorské heslá do routera, uložené v súboroch v nešifrovanom texte a vykonávať shell príkazy. V kombinácii poskytujú voľnú cestu k úplnému ovládnutiu routera.

Zraniteľnosti Cisco

Spoločnosť Cisco opravila zraniteľnosť v softvéri Cisco IOS XE verzie 16.x s konfiguráciou rozhrania Layer 3 na MACsec MKA s použitím EAP-TLS, ktorá útočníkovi umožňuje obísť autentifikáciu a smerovať komunikáciu cez rozhranie Layer 3. To umožňuje podniknúť ďalšie útoky. Zraniteľnosť má označenie CVE-2018-15372.
Ďalšia opravená skupina zraniteľností sa nachádzala v produktoch Cisco Webex Network Recording Player for Microsoft Windows a Cisco Webex Player for Microsoft Windows. Útočníkom umožňovali na zraniteľných zariadeniach vykonávať ľubovoľný kód.
Aktualizácia existuje aj na kritickú zraniteľnosť CVE-2018-0417 umožňujúcu vzdialené zvýšenie privilégií v produkte Cisco Wireless Lan Controller Software. To je spôsobené nesprávnou analýzou špecifického atribútu „TACACS“.
Aktualizácia bola vydaná vo viacerých produktoch pod Cisco 3000 Series Industrial Security Appliance pre zraniteľnosť CVE-2018-15454, ktorá dovoľuje vykonanie DoS útoku pomocou špeciálne vytvorených SIP požiadaviek.
Závažná zraniteľnosť CVE-2018-15452, ktorá ešte nebola opravená, existuje v produkte Cisco AMP for Endpoints 6.1(7). Dovoľuje lokálne vykonávať kód, pretože nevhodne narába s načítavaním DLL knižníc.

Zraniteľnosť VMware

Spoločnosť VMware opravila v niekoľkých svojich produktoch zraniteľnosť CVE-2018-6977, umožňujúcu vykonávať DoS útoky. Zraniteľné produkty sú:
VMWare Esxi 6.0, 6.5, 6.7
VMWare Fusion 10.0, 10.1, 10.1.1, 10.1.2, 10.1.3, 11.0
VMWare Fusion Pro 10.0, 10.1.1, 10.1.2, 11.0
VMWare Workstation 14.0, 14.1.0, 14.1.1
VMWare Workstation Player 14.0, 14.1, 14.1.1
VMWare Workstation Pro 14.0, 14.1, 14.1.1
Pre prvé dva a štvrtý produkt bola opravená aj závažná zraniteľnosť CVE-2018-6974, ktorá dovoľuje spôsobiť lokálne pretečenie medzipamäte na halde.
Ďalšia kritická zraniteľnosť, CVE-2018-6979, umožňujúca obídenie autentifikácie bola opravená v produkte VMWare Workspace ONE Unified Endpoint Management Console.

Mesačník zraniteľností Október 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
    - Zraniteľnosť D-Link routerov
    - CMS Drupal
    - jQuery
    - Viaceré produkty Oracle
    - LibSSH

https://www.csirt.gov.sk/aktualne-7d7.html?id=167