ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Máj 2019

Vypracoval: CSIRT.SK

TLP: White

V každodennej praxi riešenia kybernetických bezpečnostných incidentov sa CSIRT.SK najčastejšie stretáva s phishingovými útokmi. Podvodníci šíria e-maily, v ktorých sa snažia rôznymi technikami vzbudiť dôveru obete a pocit naliehavosti, aby odovzdala svoje prihlasovacie údaje do e-mailovej schránky, či účtu v inej webovej službe, alebo platobné údaje z kreditnej karty. Cieľom útočníkov môže byť aj šírenie rôzneho malvéru. Stačí obeť presvedčiť, aby klikla na odkaz v e-maile, alebo otvorila prílohu. E-maily môžu posielať masovo, alebo so zameraním na istú cieľovú skupinu.

Počet phishingových útokov za minulý rok bol dvojnásobný v porovnaní s rokom 2017. Spoločnosť Kaspersky zaznamenala takmer pol miliardy pokusov o presmerovanie na phishingové domény. Spoločnosť Google zrušila 2,3 miliardy podvodných reklám, z ktorých takmer 59 miliónov smerovalo na phishingové stránky.

Útočníci sa postupom času naučili používať širokú škálu techník, trikov a psychologických ťahov. Svoj arzenál stále rozširujú a svoje znalosti medzi sebou zdieľajú. Využívajú sociálne siete, cez ktoré priamo posielajú správy (napríklad sa vydávajú za známych „youtuberov“), alebo svoje e-maily vydávajú za oficiálne notifikácie Facebooku, a podobne. Dokážu falšovať odosielateľa e-mailovej správy, aby pôsobila dôveryhodne, či skopírovať webstránku internet bankingu, alebo e-mailovej služby. Bezpečnostní výskumníci pozorovali aj rôzne kuriózne techniky falšovania URL adries. Napríklad phishingová stránka zbierajúca prihlasovacie údaje do účtov Google bola preložená cez Google Translate, aby v odkaze dominovala legitímna adresa spoločnosti Google. Alebo malvér šíriaca kampaň zameraná na zariadenia Android, majúca za cieľ krádeže bankových údajov, sa pokúšala zvýšiť dôveryhodnosť svojej webovej stránky použitím falošnej reCAPTCHA autentifikácie. Ďalším príkladom je phishingová stránka vydávajúca sa za portál Microsoft Office 365 s integrovanou živou online podporou pre posilnenie dojmu legitímnosti. A ak máte na svojom routeri zapnutú vzdialenú administráciu, používate pre ňu prednastavené a slabé heslá a neaktualizujete jeho firmvér, môžete sa ľahko stať obeťou routerového DNS phishingu. Tiež si dávajte pozor na falošnú online podporu ku rôznym softvérovým produktom. Takéto podvody sú veľmi rozšírené a často sa snažia presvedčiť obete k odovzdaniu osobných údajov, či k neopodstatneným platbám.

Ktoré prílohy e-mailov sú najnebezpečnejšie? Výskumníci spoločnosti F-Secure zdôrazňujú, aby ste si dali pozor najmä na súbory formátu ZIP (takto sa šíril napríklad ransomvér GandCrab), PDF (rôzne phishingové kampane, od American Express po lotériu Google), ISO, IMG (malvér ako AgentTesla či NanoCore RAT) a súbory Microsoft Office (DOC, XLSM – pomocou makier šíriace napríklad bankového trójskeho koňa Trickbot).

Ako sme spomenuli vyššie, útočníci veľmi dobre poznajú a zneužívajú naše sociálne a psychologické slabiny a nedokonalosti, čo označujeme ako sociálne inžinierstvo. To je dôležitou súčasťou spear phishingu, alebo phishingu zameraného na konkrétnu obeť, či úzku skupinu. Okrem špecifických oddelení v komerčných firmách (ekonomické, HR, ...) sa môžu dostať do hľadáčiku spear phishingových útočníkov aj sofistikované skupiny, ako agenti riešiaci pranie špinavých peňazí. Podvodníci sa zameriavajú najmä na štyri emócie: zvedavosť, ľútosť, strach a chamtivosť. Využívajú náš rešpekt pred autoritou a vydávajú sa za našich nadriadených. Snažia sa nás vmanipulovať do

rýchlych, nepremyslených rozhodnutí zdôrazňovaním urgentnosti situácie. Pokúšajú sa v nás vyvolať automatickú reakciu, napríklad hláškami typu „Odosielanie správy zlyhalo. Kliknite pre opätovné odoslanie.“. Využívajú tiež reakcie na neočakávané priznania, ako „S ľútosťou Vám oznamujeme, že u nás došlo k úniku hesiel. Prosím skontrolujte, či patríte k poškodeným používateľom.“, pri ktorých poľavíme našu obozretnosť.

Aby ste sa nestali obeťou phishingu, pred zadaním citlivých údajov:

- Overte, že stránka používa šifrovaný protokol (https://) a má platný certifikát na svoje meno.
- Všímajte si nezvyčajné detaily na webstránke, ako nefunkčné položky, ktoré by mali byť rozkliknuteľné, či zvláštne vyskakovacie okná.
- Všímajte si, či odkazy naozaj vedú na stránky, na ktoré majú viesť. Kontrolujte skutočné prelinkovanie, ktoré sa zobrazí v dolnej časti prehliadača, keď prejdete myšou na položku s odkazom.
- Ak ste na známej webstránke, všimnite si, či súhlasí adresa. Podvodníci niekedy používajú znaky rôznych jazykov, ktoré pripomínajú anglickú abecedu, no často majú niečo navyše, napríklad čiarku, či háčik na spodku písmena.
- Aktualizujte pravidelne svoj router, nepoužívajte prednastavené a slabé heslá do administrátorského rozhrania a nenechávajte toto rozhranie prístupné z internetu.
- Nepoužívajte rovnakú profilovú fotku a prezývku na súkromných a pracovných účtoch.
- Nezverejňujte o sebe zbytočne veľa informácií na sociálnych sieťach.
- K príliš dobre vyzerajúcim ponukám služieb a tovaru pristupujte obozretne.

CSIRT.SK vám želá príjemné leto. A nenechajte sa nalákať na podvodné ponuky ubytovania. Vždy je podozrivé, ak vás majiteľ ubytovania inzerujúci napríklad na portáli AirBnB kontaktuje s výzvou kliknúť na nejaký odkaz...

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci máj riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Okrem toho riešil medializovaný bezpečnostný kybernetický incident na Ministerstve zahraničných vecí do tej miery, ako mu dovoľovali pridelené kompetencie a miera utajenia informácií o incidente.

V rámci proaktívnej činnosti vykonal CSIRT.SK v mesiaci máj testovanie zariadení svojej konštituencie. Svoju konštituenciu informoval o výsledkoch. Mnohé inštitúcie reagovali promptne a niektoré si vyžiadali retest po implementovaní opráv. Svoju konštituenciu tiež informoval o kritickej zraniteľnosti CVE-2019-0708, ktorá v systémoch MS Windows umožňuje šírenie malvéru cez protokol RDP bez pričinenia používateľa („worming“).

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

CSIRT.SK sa v mesiaci máj zúčastnil na celoeurópskom cvičení CyberSOPEX 2019 tematicky zameranom na voľby do parlamentu EÚ. V súvislosti s eurovoľbami a zvýšeným rizikom kybernetických útokov bol dňa 25.5.2019 v pohotovosti.

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

Významné útoky vo svete

Účty Office 365 kompromitované a využívané pri ďalších útokoch od spear phishingu po šírenie malvéru.

Útočníci pomocou phishingu, vydávajúc sa za rôzne dôveryhodné spoločnosti ako Microsoft, získali v priebehu jedného mesiaca prístup do účtov služby Microsoft Office 365 asi 4000 používateľov. Tieto použili pre ďalšie útoky typu spear phishing, šírenie malvéru a kompromitácia firemných e-mailových účtov. Z ovládnutých účtov rozposielali podvodné a škodlivé e-maily. Prístupy získali phishingom, no tiež využitím starších únikov dát. Pozorované boli aj brute-force útoky.

Útoky Magecart zamerané na krádeže údajov z platobných kariet v online obchodoch už nie sú hrozbou len pre platformu Magento.

Krádeže údajov z platobných kariet v online obchodoch pomocou JavaScript kódu, známeho ako Magecart, už nie sú hrozbou len pre platformu Magento, ale ľubovoľnú inú e-commerce platformu. Škodlivý skript bol pozorovaný aj na stránkach postavených na platformách OpenCart, WooCommerce, či OSCommerce. Ohrozené sú aj ďalšie vrátane cloudových riešení. Skupiny Magecart napádajú aj dodávateľské siete e-shopov, vrátane používaných modulov a poskytovateľov analytických služieb. Okrem platobných údajov sa začali zameriavať aj na prihlasovacie údaje, ktoré je možné predať na čiernom trhu.

Dva veľké kriminálne obchody Valhalla a Wall Street Market na Darkwebe odpojené, 6 ľudí vo väzbe.

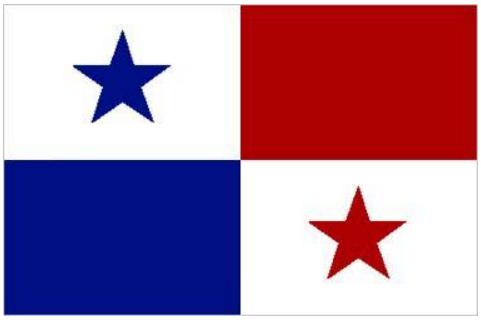
Jeden z najstarších darknetových obchodov, fínska Valhalla založená v roku 2013 ako Silkkkitie, bola odstavená fínskymi colníkmi v spolupráci s francúzskou políciou a Europolom. Ponúkala vyše 30 000 rôznych produktov, od drog po malvér a falšované dokumenty. Polícia zrušila aj nemecký obchod Wall Street Market, poskytujúci vyše 63 000 produktov od 5400

predávajúcich. Počet zákazníckych kont presahoval 1 150 000. Polícia zadržala prevádzkovateľov serverov, ktorí sa nachádzali v Nemecku, USA a Brazílii.

Ďalší hosť objavil kameru v ubytovaní poskytovanom cez AirBnB. Majiteľa nehnuteľnosti zatkli.

Žena pracujúca v oblasti IT bezpečnosti našla počas svojho pobytu v Číne vo svojom ubytovaní ukrytú kameru, keď si všimla podozrivé svetielko na wi-fi routeri. Majiteľ nehnuteľnosti poskytoval ubytovanie prostredníctvom portálu AirBnB, na ktorom získal dôveryhodný štatút „superhost“. Čínska polícia zistila, že majiteľ nahrával svojich hostí niekoľko mesiacov a zatkla ho. Podobných prípadov sa vo svete v poslednom čase vyskytlo viacero.

Nezabezpečená Elasticsearch databáza občanov Panamy odkrývala osobné údaje takmer 3,5 milióna osôb.



Nezabezpečený dátový klaster Elasticsearch obsahujúci údaje takmer 3,5 milióna občanov Panamy (90% populácie krajiny) objavil bezpečnostný výskumník Bob Diachenko. Záznamy mali označenie „pacient“ a obsahovali osobné údaje, ako mená, dátumy narodenia, čísla občianskych preukazov, adresy, čísla zdravotného poistenia a e-mailové a telefonické kontaktné údaje. Nepodarilo sa zistiť, komu klaster patrí a kto je teda za únik zodpovedný.

Únik údajov o iránskej APT skupine „Rana“ odhalil jej ciele a členov.

Na kanáli Black Box komunikačnej služby Telegram boli uverejnené utajené dokumenty, ktoré unikli z Iránu. Časť z nich je spojená s iránskou APT skupinou Rana, a obsahuje informácie o jej aktivitách, obetiach a členoch. Okrem iného hovoria plánoch útokov na letecké spoločnosti domáce aj z okolitých krajín z roku 2015 za účelom získavať informácie, na ciele v Izraeli vrátane poistných a hotelových spoločností, kuvajtské ministerstvá, a o vývoji malvéru a jeho ovládacieho rozhrania, určeného na spôsobenie škôd priemyselným SCADA systémom. Vývoj bol podľa indícií neúspešný.

TLP: White

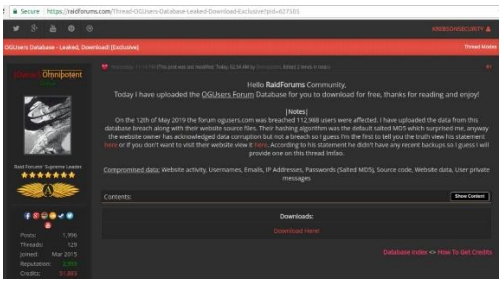
Zraniteľnosť WhatsApp zneužitá na sledovanie používateľov.

Kritickú zero-day zraniteľnosť komunikačnej aplikácie WhatsApp CVE-2019-3568 zneužili vývojári izraelskej firmy NSO Group na inštaláciu sledovacieho malvéru Pegasus do iOS a Android smartfónov obetí. Na to, aby sa malvér nainštaloval, stačí, aby útočník zavolal obeti cez aplikáciu. Obeť ani nemusí hovor zdvihnúť a príde o celú škálu citlivých údajov zo svojho telefónu. Útočníci zároveň ovládnu kameru a mikrofón smartfónu. Výskumníci spoločnosti Citizen Lab informovali, že jednou z obetí bol britský právnik zaoberajúci sa ľudskými právami.

Vyše 12 000 nezabezpečených MongoDB databáz vymazaných v priebehu troch týždňov. Útočníci Unistellar nechávajú len kontakt a odkaz „Restore?“.

Za tri týždne zo skupiny, ktorá si hovorí Unistellar, vymazali vyše 12 000 nezabezpečených databáz MongoDB, čo predstavuje asi pätinu databáz indexovaných vyhľadávačom Shodan. Štandardne sú takéto útoky vykonávané za cieľom získať výkupné za navrátenie dát obeti. Skupina Unistellar však necháva len kontaktný e-mail a odkaz „Restore?“ („Obnoviť?“). Výskumníci sa domnievajú, že to robia s cieľom vypýtať výkupné na základe dôležitosti databázy, ktorú odhadnú pri komunikácii s obeťou.

Ani kriminálne weby nie sú v bezpečí. Prienik do systémov OGUsers.



Prienik do systémov fóra OGUsers, ktoré je populárne medzi útočníkmi zameriavajúcimi sa na kompromitáciu online účty a na SIM swapping útoky, zasiahol osobné údaje 113 000 používateľov, ktoré útočníci zdarma zverejnili na konkurenčnom fóre RaidForums. Obsahovali používateľské mená, e-mailové adresy, haše hesiel, IP adresy a súkromné správy. Zároveň znamenal stratu dát na pevných diskoch. Administrátor obnovil niekoľko mesiacov starú zálohu. Používatelia stránky sú nahnevaní a majú strach, že im na dvere zaklope polícia.

Pri prieniku do systémov austrálskeho start-upu Canva ukradol útočník údaje 139 miliónov používateľov.

Útočník so pseudonymom GnosticPrayers, zodpovedný za niekoľko veľkých únikov vrátane série únikov Collection#X, spolu čítajúcich dáta až 932 miliónov používateľov, prenikol tentokrát do databáz austrálskej umeleckej start-up aplikácie Canva. Unikli údaje 139 miliónov používateľov. Okrem iného obsahovali používateľské a skutočné mená, e-mailové adresy a mestá pobytu. Unikli aj hašované heslá polovice používateľov (ktoré však boli šifrované a saltované podľa najvyšších štandardov) a istej časti aj prihlasovacie tokeny Google. Niektoré údaje patrili aj zamestnancom a administrátorom.

- **Útočníci zverejnili vyše 516 GB citlivých údajov klientov spoločnosti Citycomp po tom, čo sa spoločnosť odmietla podrobiť vydieraniu.**

- **Nájdený nový Magecart skimmer umožňujúci integráciu a krádež údajov z platobných kariet z 57 platobných brán. Už prítomný na desiatkach e-shopov založených na frameworku Magento.**

- **Minulý mesiac kompromitované e-mailové účty Microsoft Outlook, Hotmail a MSN používané na krádež kryptomien.**

- **Botnet Muhstik zneužíva na šírenie nedávno opravenú zraniteľnosť Oracle WebLogic serveru.**

- **Televízna stanica Cartoon Network napadnutá, namiesto kreslených seriálov mohli diváci sledovať brazílskeho striptéra.**

- **Únik osobných údajov vyše 100 000 osôb z nezabezpečenej Elasticsearch databázy medicínskej spoločnosti SkyMed. Sieť spoločnosti možno tiež napadnutá ransomvérom.**

- **Podvodníci vytvárajú falošné Google Search reklamy spoločností PayPal, Amazon a eBay a predstierajú, že sú zákaznícka podpora.**

- **DoS útok na neaktualizovaný systém vyvolal problémy v systémoch distribúcie elektrickej energie. Zasiahol Kaliforniu, Utah a Wyoming.**

- **Voľne dostupná databáza portálu na vyhľadávanie pracovných príležitostí Ladders poskytovala dáta 13 miliónov používateľov.**

- **Hacker ovládol 29 IoT botnetov vďaka jednoduchým či prednastaveným heslám.**

TLP: White

- Prienik do firmy PrismRBS, pozmenená e-commerce platforma PrismWeb a Magecart malvér v 201 univerzitných online obchodoch.
- Izrael bombardoval budovu s kyberútočníkmi Hamasu, čím zdecimoval ich kybernetické útočné kapacity.
- Prienik do systémov online platformy Wyzant, spájajúcej študentov s tútormi, mohol exponovať osobné údaje vyše 2 miliónov používateľov.
- Číňania používali kybernetické útočné nástroje NSA už rok pred ich únikom.
- Servery magistrátov Baltimore (Maryland) a Amarillo (Texas) napadnuté ransomvérom.
- Nechránená databáza kanadského telekomunikačného operátora Freedom Mobile exponovala finančné údaje minimálne 15 000 zákazníkov.
- 275 miliónov záznamov citlivých osobných informácií indických občanov voľne prístupných v nezabezpečenej MongoDB databáze.
- Útočníci zneužívajú servery Confluence na ťažbu kryptomien. Zneužívajú na to známe zraniteľnosti.
- 105 webstránok vrátane 6 z indexu Alexa top milión napadnutých škodlivým skriptom na krádež údajov z platobných kariet, podobným ako Magecart.
- Pacers Sports & Entertainment, spoločnosť za dvomi basketbalovými tímami z Indiany utrpela prienik do svojich systémov. Unikli citlivé osobné dáta.
- Servery 7 spoločností napadnuté škodlivým skriptom, platobné a prihlasovacie údaje zadané do tisícok webstránok exfiltrované.
- Japonské online obchody UNIQLO a GU napadnuté. Útočníci získali prístup k účtom vyše 461 000 zákazníkov. Využili „credential stuffing“, recyklované heslá.
- Osobné údaje a pasy 2,25 milióna osôb vrátane vysokých politikov ležali nezabezpečené na ruských vládnych stránkach.
- Stránka singapurského Červeného kríža napadnutá. Unikli osobné údaje vyše 4000 darcov krvi, pravdepodobne kvôli slabému administrátorskému heslu.
- Desať členov kriminálnej skupiny GozNym zadržaných pri medzinárodnej akcii. Finančným inštitúciám urobili škody 100 miliónov USD.
- Skript Magecart objavený v kóde stránky pre objednávky predplatného Forbes

Magazine.

- Údaje 8 miliónov osôb, zadané na dotazníkových stránkach, prístupné cez nechránenú Elasticsearch databázu.
- Pokles aktivity hacktivitov Anonymous od roku 2015 o 95%. Dôvodom je rozpad na frakcie, aj zatýkanie.
- Prienik na servery stránky Stack Overflow. Unikla časť dáta malého množstva používateľov.
- Systémy Paterson Public Schools v New Jersey napadnuté. Unikli prihlasovacie údaje vyše 23 000 používateľských účtov.
- Milióny osobných a prihlasovacích údajov golfových hráčov vystavených v nezabezpečenej Elasticsearch databáze aplikácie Game Golf.
- Firemné poddomény HCL Technologies (Hindustan Computers Limited) ponechávali nechránenú pestrú škálu citlivých údajov zamestnancov aj zákazníkov.
- Bankový trójsky kôň Trickbot infikoval školský obvod v Ohiu, študentov poslali domov, preinštalovať bolo treba vyše 1000 zariadení.
- Poisťovňa First American Financial Corp. exponovala na internet vyše 885 miliónov citlivých dokumentov.
- Exponovaná Elasticsearch databáza firmy Amazingco poskytovala prístup k vyše 212 000 citlivým záznamom o organizovaných akciách, vrátane osobných údajov klientov.
- Prienik do databáz webstránky Flipboard stál osobné údaje a tokeny 100 miliónov používateľov.
- 50 000 serverov MS-SQL a PHPMyAdmin infikovaných počas kampane Nanshou zameranej na ťažbu kryptomien.
- Fastfoodové reštaurácie Checkers' a Rally's infikované POS malvérom. Zasiahnutých 102 pobočiek, čo predstavuje 15% prevádzok.
- 85GB bezpečnostných logov hotelových sietí Marriott, Plaza, Sheraton, Hilton a ďalších hotelov exponovala nezabezpečená Elasticsearch databáza.
- Nezisková organizácia People Inc. zaznamenala prienik do svojich systémov a odcudzenie osobných údajov klientov. Vektorom útoku bol e-mailový účet zamestnanca.

Závažné zraniteľnosti bežných softvérových produktov

Nedôveryhodné podpisy v e-mailových klientoch

Zraniteľnosti pri overovaní e-mailových podpisov v implementáciách OpenPGP a S/MIME dovoľujú vo viacerých bežne používaných e-mailových klientoch útočníkom presvedčivo falšovať podpisy správ, a tak presvedčiť svoje obete, že prijaté správy pochádzajú od dôveryhodného zdroja. Bezpečností výskumníci kategorizovali päť druhov útokov na autentifikáciu e-mailov kryptografickým podpisom.

Zraniteľnosť na serveri Apache Tomcat umožňuje prevziať kontrolu nad zariadením

Na serveri Apache Tomcat v servlete Common Gateway Interface bola nájdená zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu. Zraniteľnosť súvisí so spôsobom, akým Java Runtime Environment (JRE) odovzdáva argumenty pre príkazový riadok operačného systému Windows. Útočník môže ovládnuť Windows server, na ktorom beží zraniteľná verzia Apache Tomcat.

Varovanie pre organizácie používajúce SAP aplikácie

Až 90% inštancií SAP systému vo svete používa nesprávnu konfiguráciu prístupových pravidiel umožňujúcu útočníkom registrovať ľubovoľné nové aplikačné servery. To môže viesť až ku prevzatiu kontroly nad zraniteľnými systémami. Nakoľko minulý mesiac výskumníci zverejnili ukážkový kód na zneužitie tejto zraniteľnosti, počet útokov na zraniteľné systémy SAP stúpa.

DELL - predinštalovaný nástroj SupportAssist umožňuje vzdialene vykonávať kód

Kritická zraniteľnosť v nástroji Dell SupportAssist, ktorý je predinštalovaný na väčšine Dell počítačov, umožňuje útočníkom nahrať a vzdialene vykonávať na zraniteľnom zariadení ľubovoľný kód. To môže viesť až ku prevzatiu kontroly nad zariadením. Nástroj sa preto odporúča bezodkladne aktualizovať, alebo odinštalovať.

Kritická zraniteľnosť Windows - zneužiteľné RDP na voľné šírenie malvéru

Kritická zraniteľnosť v operačnom systéme Windows / Windows Server sa nachádza v službe Remote Desktop Services. Neautorizovanému útočníkovi umožňuje bez interakcie používateľa vzdialene vykonávať kód a prevziať plnú kontrolu nad zraniteľným zariadením. Obdobná zraniteľnosť umožnila v roku 2017 šírenie ransomvéru WannaCry.

Kaspersky - zraniteľné sú aj antivírusy

Bezpečnostní výskumníci z tímu Imaginary objavili zraniteľnosť, ktorá sa vyskytuje v antivírovom programe spoločnosti Kaspersky Lab a umožňuje vykonávanie ľubovoľného kódu v kontexte aplikácie.

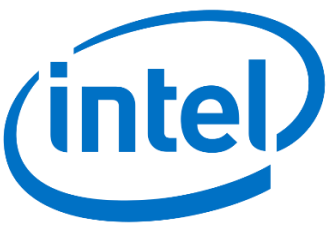
Kritická zraniteľnosť v Linux Kernel

V implementácii protokolu TCP/IP linuxového jadra sa nachádza zraniteľnosť, ktorá použitím odalokovanej pamäte umožňuje vzdialene vykonávať na zraniteľnom zariadení ľubovoľný kód.

Zraniteľnosti v PrintLogic dovoľujú útočníkom meniť konfiguračné súbory a vzdialene vykonávať kód

V softvéri PrintLogic Management boli objavené tri zraniteľnosti umožňujúce vzdialene vykonávať ľubovoľný kód a upravovať konfiguračné súbory programu. Útočníci to môžu dosiahnuť predstieraním cudzej identity, DNS spoofingom, modifikovaním sťahovaného kódu, či vkladaním špeciálnych znakov do webového prehliadača, z ktorého vstupy program nekontroluje.

Nové zraniteľnosti procesorov Intel



Bezpečnostní výskumníci objavili viacero zraniteľností procesorov Intel. Milióny počítačov sú v ohrození. Zraniteľnosti umožňujú čítať citlivé údaje vrátane hesiel, tokenov a histórie webových prehliadačov, zneužitím bočného kanála pri vykonávaní špekulatívnej exekúcie. Aplikácia opráv spôsobí zníženie výkonu procesorov, ktorého veľkosť záleží od ich konkrétnej aplikácie.

TLP: White

Najviac zasiahnuté budú pravdepodobne dátové centrá. Vzhľadom na povahu zraniteľností sa predpokladá cielené zneužívanie, nie plošná kampaň.

Windows 10 zero-day zraniteľnosť od SandboxEscapera

Výskumník s pseudonymom SandboxEscaper zverejnil ďalší ukážkový kód na zneužitie zero-day zraniteľnosti v systéme Windows 10. Zraniteľnosť sa nachádza v nástroji Task Scheduler a dovoľuje útočníkom zvýšiť práva až na úroveň systému. Následne je možné vykonávať ľubovoľný kód s právami systému. Na zraniteľnosť zatiaľ neexistuje opravná aktualizácia.

Zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Elastic Services Controller (CVE-2019-1867): kvôli nesprávnej validácii REST API požiadaviek dochádzalo k obídeniu autentifikácie.
Cisco IOS XE (CVE-2019-1862): zraniteľnosť vo webovom používateľskom rozhraní umožňovala autentifikovanému útočníkovi vzdialene vykonávať príkazy s právami root v Linuxovom prostredí, na ktorom aplikácia bežala. Dôvodom bola nesprávna kontrola používateľských vstupov.
Cisco IOS XR pre *Cisco Aggregation Service Router 9000 Series* (CVE-2019-1846): kvôli nesprávnemu narábaniu s paketmi MPLS OAM mohol neprihlásený útočník vyvolať DoS podmienky a zhodiť proces lspv_server.
Cisco Nexus 9000 Series ACI (CVE-2019-1804): zraniteľnosť v správe SSH kľúčov umožňovala neautentifikovanému vzdialenému útočníkovi pripojiť sa k systému s právami root. Toto bolo možné cez IPv6 vďaka prítomnosti predinštalovaného rovnakého SSH kľúča vo všetkých zariadeniach.
Cisco Secure Boot (CVE-2019-1649): zraniteľnosť viacerých hardvérových zariadení Cisco s podporou Secure Boot. Autentifikovaný útočník mohol nahrať modifikovaný firmvér do zraniteľného zariadenia za rôznym účelom.
Cisco Prime Infrastructure / Evolved Programmable Network Manager (CVE-2019-1821, CVE-2019-1822, CVE-2019-1823): kvôli nesprávnemu vyhodnocovaniu používateľských vstupov mohol útočník nahrať do administratívneho webového prostredia škodlivý súbor a vykonávať tak kód s právami root.
Cisco Video Surveillance Manager (CVE-2019-1717): kvôli nesprávnemu vyhodnocovaniu parametrov vo webovom manažovacom rozhraní mohol útočník odoslaním špeciálnej požiadavky stiahnuť zo zariadenia ľubovoľný súbor.

Cisco Nexus 3000 / 9000 Series (CVE-2019-1810): kvôli nevhodnému overovaniu digitálneho podpisu softvéru počas vykonávania CLI príkazov mohlo dochádzať k obídeniu bezpečnostných prvkov. Autentifikovaný útočník mohol do zariadenia inštalovať nepodpísaný softvér.

Zraniteľnosť Oracle WebLogic Server

V aplikačnom serveri Oracle WebLogic Server bola opravená kritická zraniteľnosť CVE-2019-2725, ktorá umožňovala vzdialené vykonávanie príkazov kvôli deserializácii vstupov. Týkala sa komponentov wls9_async a als_wsat. Útočník mohol vykonávať vzdialene príkazy s právami práve prihláseného používateľa.

Chyba Palo Alto Networks Demisto

Systém Palo Alto Networks Demisto mal zraniteľnosť CVE-2019-1568 umožňujúcu vykonávať cross-site scripting útoky kvôli nesprávnemu vyhodnocovaniu používateľských vstupov. Útočník mohol vykonávať ľubovoľný kód v prehliadači obete a napríklad odcudziť autentifikačné súbory cookie.

Zraniteľnosti VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
VMware Workstation (CVE-2019-5526): kvôli nesprávnemu vyhodnocovaniu vstupov pred načítaním DLL súborov bolo možné vzdialene vykonávať kód s administrátorskými právami.
VMware produkty (CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091): v produktoch firmy VMware existovali zraniteľnosti spojené so zraniteľnosťami procesorov Intel s názvom „Micro-architectural Data Sampling“ (MDS). Útočník s možnosťou vykonávať lokálne kód mohol získavať údaje inak chránené architektúrou procesora.

Zraniteľnosť SQLite

Kritická zraniteľnosť v SQLite (CVE-2019-5018) umožňovala vzdialene vykonávať kód kvôli chybe použitia odalokovaného miesta v pamäti. Útočník mohol zraniteľnosť zneužiť odoslaním špeciálne vytvorenej SQL požiadavky.

Zraniteľnosť McAfee Endpoint Security

Kritická zraniteľnosť McAfee Endpoint Security (CVE-2019-3586) umožňovala obchádzanie bezpečnostných prvkov. Chyba sa nachádzala vo firewalle, ktorý nedokázal vhodne blokovať IP adresy označené ako Global Threat Intelligence. Útočníci mohli pomocou špeciálne vytvorených webstránok obchádzať niektoré bezpečnostné obmedzenia.

Chyba Wireshark

Kritická zraniteľnosť CVE-2019-12295 v aplikácii Wireshark umožňovala útočníkom spôsobiť DoS podmienky injektovaním upraveného paketu, ktorý spôsobil pás aplikácie. Chyba sa nachádzala v súbore „epan/packet.c“.

Zraniteľnosť v technológii Docker

Kritická zraniteľnosť CVE-2019-15664 sa nachádzala vo všetkých verziách kontajnerovej technológie Docker, konkrétne vo funkcii FollowSymlinkInScope, ktorá rozpoznáva zadanú cestu k súboru. Ak útočník podvrhne upravenú cestu, môže zvýšiť svoje práva na root a napríklad pomocou funkcie „docker cp“ získať právo na čítanie a zápis súborov do ľubovoľnej cesty na hostiteľskom systéme.

Mesačník zraniteľností Máj 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
    - Windows 10 Task Scheduler
    - Windows RDS
    - Zraniteľnosti procesorov Intel
    - PrintLogic
    - Linux Kernel
    - Kaspersky
    - SAP
    - Dell SupportAssist
    - Podpisy v e-mailových klientoch
    - Apache Tomcat

https://www.csirt.gov.sk/aktualne-7d7.html?id=190