ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Január 2019

Vypracoval: CSIRT.SK

TLP: White

Kto by pred desiatimi rokmi povedal, že neprejde dlhá doba a bude možné hacknúť dokonca stavebný žeriav? Tím výskumníkov zo spoločnosti Trend Micro sa pozrel na zúbok rádiovo ovládaným žeriavom a inej ťažkej technike od niekoľkých výrobcov. Vykonal laboratórne testy aj testy na skutočnej technike. Títo páni zistili, že všetky testované zariadenia boli zraniteľné voči niekoľkým druhom útokov, pretože komunikácia medzi ovládačom a prijímačom nebola chránená. Dokázali napríklad odchytiť rádiový signál a s úspechom ho opätovne odoslať mechanizmu ako pokyn. Taktiež bolo možné odchytiť signál a zariadeniu ho odoslať až po úprave, čo v praxi znamená úplnú kontrolu útočníka nad ťažkým zariadením. Na zariadenia bolo možné previesť tiež DoS útok opakovaným odosielaním signálu pre núdzové zastavenie, spárovať vlastný kontrolér s prijímačom a odpojiť legitímny kontrolér, či prepísať firmvér zariadenia svojim programom. Pokiaľ útočník umiestni malé batériou napájané zariadenie v dosahu mechanizmu, nepotrebuje byť fyzicky v jeho blízkosti a útoky môže vykonávať cez internet.

Rádiové ovládanie ťažkých stavebných mechanizmov zďaleka nie je jedinou zraniteľnou skupinou v priemysle a kritickej infraštruktúre. Správy o zraniteľnostiach takýchto zariadení sa objavujú pravidelne. Tento mesiac napríklad boli objavené dve závažné zraniteľnosti v priemyselnej meteostanici od spoločnosti ControlByWeb, ktorá môže byť integrovaná so SCADA systémami (Supervisory Control and Data Acquisition). Na zariadenie je tak možné vykonať DoS útok a cez XSS útok vložiť škodlivý skript. Taktiež sú už nejakú dobu známe zraniteľnosti programovateľných logických kontrolérov (PLC), pričom ako bonus pre útočníkov slúžia zneužiteľné ich legitímne vlastnosti. Napríklad softvérový inžinier Roee Stark ukázal, ako je možné zneužiť funkcionalitu protokolu CIP (Common Industrial Protocol) na kontroléroch od Rockwell Automation. Útočník s prístupom ku kontroléru dokáže vzdialene zbierať dáta, alebo preniknúť hlbšie do internej siete a ovládať ďalšie pripojené kontroléry vo výrobe.

Mimo priemyselných systémov sú často nedostatočne implementované bezpečnostné opatrenia aj v kritickej infraštruktúre. Jedným príkladom je americký systém protiraketovej obrany, ktorého mnohé zariadenia takmer päť rokov neimplementovali vyžadované opatrenia, akými sú dvojfaktorová autentifikácia, šifrovanie dát ukladaných na prenosné médiá, či zamknuté dvere a bezpečnostné kamery v serverovniach. Americká vláda si pritom uvedomuje rastúce riziká pre kritickú infraštruktúru, vrátane energetiky, úpravy vody, ropného a plynárenského priemyslu a obrany. Správa amerických tajných služieb Worldwide Threat Assessment hovorí, že najväčšími rizikami pre kritickú štruktúru USA a ich spojencov sú Čína a Rusko, no aj Irán sa tiež pokúša vyvinúť možnosti na takýto druh kybernetického útoku. Nezanedbateľnými hráčmi sú aj Severná Kórea, teroristické organizácie a kyberzločinci bažiaci po zisku.

Spoločnosť Kaspersky Lab vydala štúdiu, v ktorej spomína, že v prvej polovici roka 2018 bolo 41,2% priemyselných kontrolných systémov napadnutých malvérom. Množstvo útokov v čase narastá. Netýka sa to len Spojených štátov. Aj talianska ropná a plynárenská spoločnosť Saipem koncom minulého roka zažila veľký útok malvérom Shamoon, ktorý zničil dáta na približne 10% počítačov. Spoločnosť mala našťastie nastavenú politiku zálohovania dát. Pred niekoľkými rokmi pri podobnom

útoku prišla saudská ropná spoločnosť Aramco o množstvo dát. Zaznamenané boli aj cielené manuálne útoky ransomvérom s veľkým dopadom.

Spôsob akým často útočníci postupujú pri útokoch na kritickú infraštruktúru, popísala štúdia Vectra 2018 Spotlight Report on Energy and Utilities. V skratke najprv kompromitujú podnikovú IT sieť spoločnosti, kde sledujú operátorov, získavajú informácie a prístupy pre druhú fázu. Priemyselnú špionáž je možné vykonávať napríklad aj s pomocou rozšírení pre internetové prehliadače, alebo trebárs malvérom v softvéri AutoCAD. Táto fáza a plánovanie ďalšieho útoku trvajú typicky mesiace. Následne zaútočia na ICS (priemyselné kontrolné systémy).

Priemysel a kritická infraštruktúra si niekoľko rokov trvajúcu bezpečnostnú situáciu začína uvedomovať a spoločnosti podnikajú potrebné kroky. Napríklad Schnieder Electric, ktorá poskytuje architektúru a platformu EcoStruxure IoT, spolupracuje na zabezpečení svojich riešení s niekoľkými bezpečnostnými spoločnosťami (Nozomi, Entrust Datacard, Claroty, McAfee, Waterfall Security).

Niekoľko užitočných rád, ako znížiť riziko úspešného útoku na organizácie priemyslu a kritickej infraštruktúry, znie pravdepodobne povedome:

- Zavedenie multifaktorovej autentifikácie, najmä k administrátorským účtom, no ideálne všade vrátane súkromných účtov zamestnancov na rôznych internetových službách.
- Vyškolenie zamestnancov ohľadom phishingu a spear-phishingu, čo sú bežné cesty, ako sa malvér dostane do interného systému.
- Hardenovanie systémov, sietí a IoT zariadení, aktualizovanie
- Zosúladenie s požiadavkami NERC, FERC, ISA, ISO...
- Využívanie riešení bez agentov, aby nebol ovplyvnený výkon a dostupnosť zastaraných SCADA systémov

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci január riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu a informoval inštitúcie o závažných zraniteľnostiach (Linux APT). Tiež zaznamenal kampaň šíriacu škodlivé prílohy z kompromitovaných schránok leteckých spoločností.

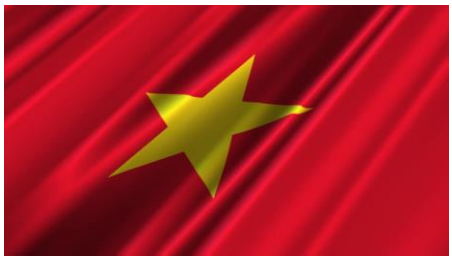
Vo svojej konštituencii CSIRT.SK zaznamenal prítomnosť spyware HawkEye Keylogger – Reborn v9.

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

Okrem toho CSIRT.SK študoval prekryv uniknutej veľkej databázy zozbieraných uniknutých párov e-mailových adries a hesiel zväčša vo voľnom texte, nazvanej „Collection #1“ - „Collection #5“, s e-mailovými kontaktmi svojej konštituencie. Celkovo unikli miliardy prihlasovacích údajov, medzi ktorými boli nájdené aj .gov.sk adresy. CSIRT.SK rozposlal informáciu o úniku prihlasovacích údajov svojej klientele a odporučil zmenu hesiel.

Významné útoky vo svete

Ohrozenie používateľských dát vo Vietname



Vietnamská socialistická republika schválila zákon, ktorý nariaďuje internetovým spoločnostiam mazať obsah, ktorý vláda považuje za protištátny. Zákon si vyslúžil silnú kritiku USA, EU a ďalších strán a bol spojený s cenzúrou internetu, aká existuje v Číne. Zákonu sa v krajine musia podriadiť aj nadnárodné spoločnosti ako Facebook a Google.

Tisíce smart TV zariadení napadnuté kvôli reklame PewDiePie

Hacker so pseudonymom TheHackerGiraffe zodpovedný za minulomesačnú tlačiarňovú kampaň na podporu youtubera PewDiePie opäť šíril podobnú reklamu. Tentokrát si vybral zariadenia smart TV, Chromecast a Google Home, ktoré boli pripojené cez nesprávne nakonfigurované routre s povolenou funkcionalitou UPnP.

Poskytovateľ cloud hostingu napadnutý ransomvérom

Spoločnosť DataResolution.net, poskytujúca cloud hostingové služby asi 30 000 spoločnostiam po celom svete, utrpela infekciu ransomvérom Ryuk na Štedrý večer 2018 a v januári obnovovala svoje systémy. Útočníci získali kontrolu nad doménou datacentra spoločnosti. Spoločnosť odstavila svoju sieť aby zabránila šíreniu ransomvéru a obnovila svoje systémy.

Exponované dáta 2,4 milióna používateľov správcu hesiel Blur

Spoločnosť Abine dokončila bezpečnostný audit kvôli prieniku do ich systémov, ktorý sa odohral v decembri minulého roka. Rozsah úniku dát zasiahol 2,4 milióna používateľov ich produktu Blur password manager. Z nevhodne zabezpečeného Amazon S3 úložiska unikli e-mailové adresy, mená, nápovedy k heslám, IP adresy posledných prihlásení a zašifrované heslá. Spoločnosť

pre istotu navrhla používateľom zmeniť si heslá.

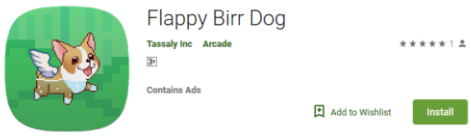
Únik údajov 7,6 miliónov hráčov hry Town of Salem

Koncom minulého roka došlo k prieniku do systémov spoločnosti BlankMediaGames (BMG) prevádzkujúcej populárnu online hru Town of Salem. Unikli údaje 7,6 milióna používateľov, ktoré okrem iného obsahovali mená, e-mailové adresy, IP adresy, heslá a záznamy o užívateľskej aktivite. O prieniku informovala služba DeHashed, kam boli dáta nahrané. Spoločnosť BMG začiatkom roka zabezpečila zasiahnuté serveri a odstránila z nich niekoľko zadných vrátok. Používatelia hry Town of Salem si môžu skontrolovať, či unikli ich údaje, aj na službe Have I Been Pwned.

Prienik do systému prevádzkovateľa Dublinských električiek

Operátor dublinských električiek, spoločnosť Luas, utrpela útok na svoju webstránku a únik dát. Útočník na webstránku spoločnosti umiestnil požiadavku na výkupné jeden Bitcoin za to, že neuverejní citlivé dáta zákazníkov spoločnosti. V požiadavke tiež stálo, že pred časom spoločnosť kontaktoval a oznámil im vážne bezpečnostné nedostatky. Útočníka k činu vyprovokovala pasivita Luas, ktorá na správu nereagovala.

Malvér z Google Play zasiahol 100 000 obetí v 196 krajinách



Malvér typu spyware zameraný na operačný systém Android ukryli útočníci do 6 hier a utilít a nahrali na repozitár Google Play. Jedna z nich, Flappy Birr Dog, pretrvala na repozitári vyše roka, až do začiatku 2019. Spoločnosť Trend Micro v spomínaných aplikáciách našla malvér ANDROIDOS_MOBSTSPY, ktorý dokáže exfiltrovať zo zariadenia polohu, súbory a SMS správy a podvrhnúť obeti phishingové vyskakovacie okná pre získanie prihlasovacích údajov do účtov na Google a Facebooku. Rozsah známych škôd je 100 000 obetí v 196 krajinách sveta.

Dáta nemeckých politikov na Twitteri

Útočníci získali osobné dáta stoviek nemeckých politikov z ľavicových a stredových strán, a tiež umelcov a youtuberov, ktoré propagovali cez Twitter. Dáta pravdepodobne získali zo smartfónov obetí. Dáta obsahovali mená, adresy, telefonické a e-mailové kontakty, identifikačné aj osobné fotografie a históriu osobných správ. Časový rozsah dát je medzi rokmi 2012 a 2018.

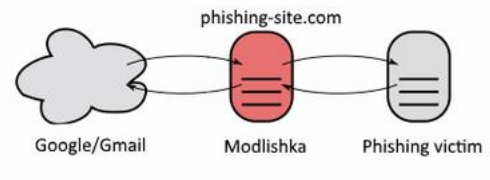
Útočníci rok kradli platobné údaje zákazníkov Titan Manufacturing and Distributing

Od novembra 2017 do októbra 2018 bol v systéme spoločnosti Titan Manufacturing and Distributing aktívny malvér, ktorý z online obchodu kradol údaje zákazníkov vrátane mien, fakturačných adries, telefónnych čísiel a údajov o platobných kartách. Spoločnosť spolupracuje s externým subjektom na vyšetrení incidentu a zabezpečení svojich systémov. Charakteristiky útok naznačujú, že za ním stojí niektorá zo skupín Magecart.

Spoločnosť OXO zasiahnutá skriptom Magecart

Výrobca kuchynských potrieb OXO International informovala o prieniku do svojich systémov, ktorý pretrvával od júna do konca novembra 2018. V stanovisku sa hovorí, že forenzné vyšetrovanie potvrdilo, že údaje, ktoré zákazníci zadali do online obchodu, mohli byť kompromitované. Vyšetrovanie spoločnosti BleepingComputer odhalilo, že sa jednalo o infekciu skriptom Magecart.

Automatizovaný phishing obchádza 2-faktorovú autentifikáciu



Poľský bezpečnostný výskumník Piotr Duszyński vytvoril nástroj na penetračné testovanie Modlishka, ktorý dokáže automatizovať phishingové kampane a dokáže prekonať 2-faktorovú autentifikáciu (2FA). Modlishka funguje ako reverzný proxy server s phishingovou doménou medzi obeťou a webstránkou (napr. Gmail). Obeť zadá prihlasovacie údaje na phishingovú doménu, ktorá ich zaloguje a posunie legitímnej webstránke.

Následne si vypýta kód 2FA, ktorý útočník môže použiť na prihlásenie. Phishingová stránka využívajúca nástroj Modlishka nepotrebuje napodobeninu legitímnej webstránky, pretože si jej obsah stiahne a ukáže obeti. Útočníkovi teda stačí doména a platný TLS certifikát, aby nevzbudil podozrenie u obete. Nástroj nedokáže obísť U2F autentifikáciu pomocou hardvérového prvku.

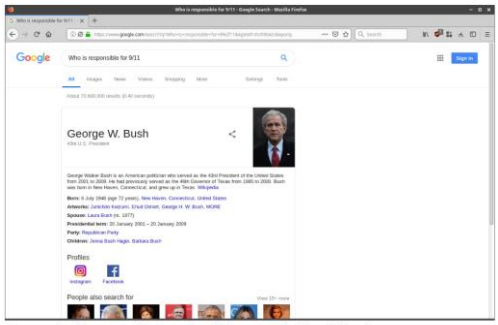
DNS hijacking kampaň zasahuje spoločnosti po celom svete

Bezpečnostná spoločnosť FireEye informovala o kampani majúcej za cieľ preberanie kontroly nad DNS záznamami, ktorú pozoruje of začiatku roku 2017. Obeťami sú vládne organizácie, poskytovatelia internetu a telekomunikačné spoločnosti z oblasti Stredného východu, severnej Afriky a Severnej Ameriky a Európy. Niekoľko indícií poukazuje na skutočnosť, že sa pravdepodobne jedná o kampaň Iránu.

Exponovaná MongoDB databáza s vyše 200 miliónmi životopisov

Bezpečnostný výskumník Bob Diachenko objavil exponovanú nezabezpečenú MongoDB databázu obsahujúcu približne 200 miliónov životopisov uchádzačom o prácu z Číny. Životopisy obsahovali osobné a kontaktné údaje uchádzačov. Tento materiál by bolo možné zneužiť na cielenú phishingovú kampaň. Z internetu bol prístup znefunkčnený o týždeň.

Výsledky vyhľadávania Google sfalšované na šírenie falošných správ



An example of how easy it is to produce fake news using Google Search.

Holandský výskumník Wietze Beukema odhalil techniku, ktorá umožňuje ovplyvňovať výsledky vyhľadávania Google, a tak tvoriť falošné správy, dezinformácie, či politickú propagandu. Dajú sa na to použiť tzv. „Knowledge Cards“ nachádzajúce sa napravo na vyhľadávacej obrazovke. Napriek ich nedokonalosti ich mnoho ľudí pokladá za dôveryhodný zdroj informácií. Problémom však je, že hocikto môže nastaviť ľubovoľnú takúto kartu k svojej vyhľadávacej fráze a tak spojiť aj nesúvisiace informácie. Útočník môže tiež vytvoriť vyhľadávaciu adresu ktorá ukáže len kartu, bez výsledkov vyhľadávania, čo podporí vieru obete

v pravdivosť spojenia týchto dvoch informácií. Spoločnosť Google na odstránení problému pracuje.

Predinštalovaný malvér na smartfónoch Alcatel

Stotisíce mobilných telefónov Alcatel, najmä modelov Pixi 4 a A3 Max boli obeťami malvéru skrytého v aplikácii Weather Forecast-World Weather Accurate Radar od spoločnosti TCL Corporation. Infikovaná bola predinštalovaná verzia, ako aj verzia dostupná na Google Play. Malvér sa pokúšal zaregistrovať používateľov na platené telefónne čísla, v pozadí spúšťal reklamy a klikal na ne, a tiež odosielal používateľské dáta na server v Číne. Na problém prišla bezpečnostná spoločnosť Upstream a zatiaľ nie je známe, akým spôsobom sa malvér do aplikácie dostal.

Milióny exponovaných SMS správ a záznamov hovorov

Justin Paine zo spoločnosti CloudFlare objavil voľne dostupnú ElasticSearch databázu patriacu spoločnosti VOIPo, poskytujúcej VoIP služby. Databáza obsahovala 4 roky záznamov vrátane 6,7 miliónov záznamov hovorov, 6 miliónov SMS a MMS a 1 milión záznamov obsahujúcich API kľúč pre interné systémy. Spoločnosť zabezpečila svoju databázu v deň, keď bola na jej exponovanosť upozornená.

Stovky online obchodov napadnuté kódom kradnúcim platobné údaje

Útok skupiny Magecart 12 zasiahol 277 online obchodov a prešetrované sú tisíce ďalších. Skupina prenikla do systému francúzskej reklamnej spoločnosti Adverline a pomocou siete reklamných slotov na stránkach v ich sieti rozšírila JavaScript kód kradnúci platobné údaje do internetových obchodov. V súčasnosti útočné domény nefungujú. Koncový používateľ má málo možností ako sa útokom typu Magecart brániť. Jedným spôsobom je vypnúť počas nákupu JavaScript. Ak to znemožní fungovanie internetového obchodu, ostáva využiť napríklad niektorú službu poskytujúcu jednorazové virtuálne platobné karty.

Kompromitácia služby Amadues zasahuje 141 leteckých spoločností

Výskumníci zo spoločnosti Safety Detective objalivi zraniteľnosť v bookovacom systéme Amadeus, kde je možné kúpiť letenku od 141 medzinárodných leteckých spoločností. Predstavuje to 44% svetového trhu. Výskumníci sa dostali do systému, kde mohli získavať osobné údaje cestujúcich a meniť parametre ich rezervácií. Spoločnosť Amadeus už zraniteľnosť odstránila.

Milióny vládnych spisov Oklahomy exponované na internete

Ďalší nezabezpečený server. Tentokrát patriaci Oklahoma Department of Securities, umožňoval voľný prístup k miliónom citlivých dokumentov od vyšetrovacích spisov FBI, cez údaje finančných brokerov a pacientov s AIDS, až po prihlasovacie údaje na vzdialené prihlásenie na servery Oklahoma Department of Securities. Dokumenty boli dostupné týždeň a hneď po ohlásení bol server zneprístupnený. Potenciálne mohli uniknúť 3 TB citlivých dokumentov od roku 1986.

Krádež vojenských záznamov Južnej Kórei

Defense Acquisition
Program Administration

Ministerstvo obrany Južnej Kórei sa stalo cieľom útočníkov, ktorí prenikli do 30 počítačov a ukradli citlivé dáta z 10 z nich. Počítače patrili agentúre pre dohľad nad akvizíciami zbraní a munície. Podľa informácií sa útočníci dostali do systému cez bezpečnostnú aplikáciu, ktorá má paradoxne zabraňovať sťahovaniu dokumentov z vládnych počítačov.

Miliardy prihlasovacích údajov dostupných na darkwebe

Bezpečnostný výskumník Troy Hunt upozornil na objav obrovskej databázy e-mailov a hesiel na darkwebe rozdelenej do niekoľkých zložiek s názvom Collection #1 - #5 o celkovej veľkosti takmer 1 TB. Databáza obsahuje miliardy záznamov a pozostáva z väčšieho množstva starších únikov. Indície naznačujú, že najstaršie údaje sú ešte z roku 2008. Troy Hunt však spomenul informáciu naznačujúcu, že niektoré môžu byť len z novembra

2018. Užívatelia, ktorí dlhodobo používajú svoje heslá, si môžu overiť ich únik na webstránke Have I Been Pwned a v prípade pozitívneho nálezu zmeniť na všetkých službách, kde ich používajú.

Pretrvávajúce útoky na západoafrické finančné inštitúcie

Výskumníci spoločnosti Symantec informovali, že od polovice roku 2017 pretrváva vlna útokov na finančné inštitúcie v západnej Afrike. Napadnuté boli organizácie v Kamerúne, Kongu, Ghane, Pobreží Slonoviny a Rovníkovej Guinei. Zaznamenané boli 4 typy útokov, pričom jeden zahŕňal trójskeho koňa a nástroj PsExec, ďalší škodlivý Powershell skript, nástoj na získavanie hesiel Mimikatz a balík na penetračné testovanie Cobalt Strike, tretí Remote Access Tool (RAT) a nástroje pre Remote Desktop Protocol a posledný využíval tiež nástroj typu RAT.

Chyba v Android aplikácii roky exponovala súkromné správy na Twitteri

Twitter opravil zraniteľnosť vo svojej aplikácii pre Android, ktorá verejne exponovala súkromné správy, aj keď mali používatelia nastavenú voľbu „Protect your Tweets“. Chyba bola v aplikácii prítomná od novembra 2014. Spoločnosť informovala svojich používateľov a po opravení chyby automaticky aktivovala ochranu súkromných správ tým užívateľom, ktorí ju mali predtým zapnutú.

Webstránky môžu exfiltrovať dáta zneužitím 200 rozšírení pre prehliadače

Akademický výskumník Dolière Francis Somé publikoval štúdiu, v ktorej sa zameral na bezpečnosť rozšírení webových prehliadačov. Vzhľadom na to, že sa nemusia riadiť Same Origin Policy pravidlom ako webové aplikácie, môžu potenciálne čítať a zapisovať dáta vo webových aplikáciách. Somé zistil, že z vyše 78 000 študovaných rozšírení takmer 4 000 vykazuje podozrivé správanie. Ďalšou analýzou zistil, že 197 rozšírení, väčšinou pre prehliadač Chrome, môže byť zneužitých webovými aplikáciami a skriptami v nich na vykonávanie ľubovoľného kódu, prístup k užívateľským dátam

a sťahovanie súborov na zariadenie obete. Vývojári prehliadačov problém riešia.

Online kasínam unikli záznamy o vyše 100 miliónoch stávkach

Bezpečnostný výskumník Justin Paine objavil nezabezpečenú ElasticSearch databázu, ktorá obsahovala vyše 108 miliónov záznamov o stávkach v rôznych online kasínach. Záznamy sa okrem iného skladali z mien, adries, e-mailových kontaktov, čiastočných údajov o platobných kartách a stavených sumách, výberov a vkladov a zostatku na účte. Databáza bola krátko po oznámení jej exponovanosti zabezpečená.

100 000 malvér šíriacich stránok zrušených

Za posledných 10 mesiacov bezpečnostní výskumníci odhalili a nahlásili poskytovateľom webhostingu takmer 100 000 webstránok šíriacich malvér. Tieto boli zrušené. Slúžili najmä na šírenie trójskych koní Emotet a Gozi a ransomvéru GandCrab. Udialo sa to v rámci projektu URLhaus organizovaného neziskovou bezpečnostnou spoločnosťou Abuse.ch, do ktorého sa zapojilo 265 bezpečnostných výskumníkov.

Exponovaná databáza 24 miliónov hypoték a pôžičiek

Ďalšia nezabezpečená ElasticSearch databáza, ktorú objavil bezpečnostný výskumník Bob Diachenko, obsahovala desiatky tisíc pôžičiek a hypoték poskytnutých niekoľkými finančnými inštitúciami vrátane Wells Fargo a CapitalOne. Diachenko našiel spolu približne 24 miliónov skenov záznamov s citlivými dátami vrátane mien, adries, čísel sociálneho poistenia, histórii a veľkosti pôžičiek. Databáza patrila spoločnosti Ascension Data & Analytics zaoberajúcej sa dátovou analýzou pôžičiek a sprostredkovaním ich odkupu od bánk. Databáza bola následne zabezpečená.

Exponované tisíce databáz ruských firiem

Bezpečnostný výskumník Victor Gevers informoval, že v tisíckach nezabezpečených MongoDB databáz ruských firiem figuruje účet admin@kremlin.ru, ktorý predstavuje zadné vrátka k citlivým informáciám v nich. Štúdiom problému zistil, že Kremeľ vyžaduje vzdialený prístup do systémov narábajúcich s finančnými transakciami. Rovnaký účet našiel dokonca v MongoDB databáze ukrajinského ministerstva zahraničných vecí, ktorá obsahovala informácie o vyšetrovaní skorumpovaných politikov. Po informovaní Kremľa už Geversova skupina tento účet nevidela.

Únik citlivých údajov zamestnancov spoločnosti Airbus

Spoločnosť Airbus ohlásila prienik do systémov spojených s komerčnou časťou a únik dát svojich európskych zamestnancov. Útočníci pristúpili najmä k pracovným dátam, ako pracovné kontakty a identifikátory. Spoločnosť zamestnávajúca vyše 10 000 ľudí incident vyšetrovala a podnikla kroky pre lepšie zabezpečenie svojich systémov.

Milióny správ zákazníkov State Bank of India exponované

State Bank of India
THE BANKER TO EVERY INDIAN

SBI

Spoločnosť State Bank of India ponechala na internete voľne dostupnú databázu svojej služby Quick. Tá umožňuje klientom rýchlo cez sms, alebo hovor získať výpis z účtu a iné služby. Databáza obsahovala milióny sms správ medzi bankou a jej klientmi, telefónne čísla, zostatky na účtoch a časti čísel účtov a prehľad transakcií. Po nahlásení banka databázu do niekoľkých hodín zabezpečila, nevydala však verejné vyhlásenie.

Závažné zraniteľnosti bežných softvérových produktov

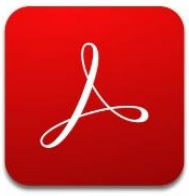
Kritická zraniteľnosť v Linuxovom správcovi APT umožňuje vzdialené vykonávanie kódu

Kritická chyba v Linuxovom správcovi balíčkov APT umožňuje pri presmerovávaní na zrkadlo útočníkovi vložiť do HTTP komunikácie upravený balíček, či škodlivý kód, ktorý správca APT vyhodnotí ako legitímny. Takto útočník dostáva možnosť vzdialene vykonávať ľubovoľný kód s právami root.

Vzdialené vykonávanie kódu v aplikácii Windows Contacts (zero-day)

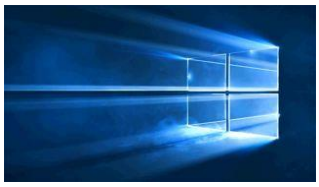
Zraniteľnosť v aplikácii Windows Contacts umožňuje útočníkovi vytvoriť škodlivú vizitku vo formáte .VCF, alebo .Contact. Keď na ňu obeť klikne, útočník môže vykonávať ľubovoľný kód s právami práve prihláseného užívateľa. Spoločnosť Microsoft neplánuje zraniteľnosť odstrániť. Záplatu vydala spoločnosť 0patch.

Dve kritické chyby v Adobe Acrobat a Reader



Spoločnosť Adobe opravila dve kritické zraniteľnosti vo svojom softvéri na tvorbu, úpravu a prehliadanie PDF súborov. Zraniteľnosť CVE-2018-16011 umožňuje použiť odalokované miesto v pamäti a následne vykonávať ľubovoľný kód s právami práve prihláseného používateľa. Zraniteľnosť CVE-2018-19725 dovoľuje obchádzať zabezpečenie a zvýšiť práva.

Bezpečnosť Windows DNS serverov ohrozuje pretečenie zásobníka



Zraniteľnosť CVE-2018-8626 spôsobuje pretečenie haldy, čo umožňuje vykonávať ľubovoľný kód na Windows serveroch nakonfigurovaných ako DNS server. Zraniteľnosť umožňuje útočníkom odosielať škodlivé požiadavky, ktoré DNS serveri nevhodne spracovávajú.

Tri závažné zraniteľnosti v produktoch Intel

Spoločnosť Intel opravila tri závažné zraniteľnosti vo svojich produktoch. Zraniteľnosť CVE-2018-12177 v nástroji na manažment bezdrôtových pripojení Intel PROset/Wireless Wi-Fi umožňuje eskalovať práva. Zraniteľnosť CVE-2019-0088 sa nachádza v produkte Intel System Support Utility for Windows, ktorý nedostatočne kontroluje cestu a umožňuje prihlásenému používateľovi eskalovať práva. Zraniteľnosť CVE-2018-18098 sa nachádza v Intel SGX platforme a taktiež dovoľuje zvýšenie práv kvôli nevhodnému spôsobu overovania súborov v inštalačnej procedúre pre Intel's SGX SDK a Platform Software for Windows.

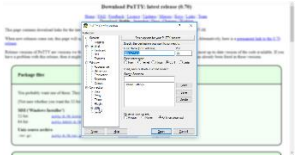
Chyba v Cisco AsyncOS umožňuje permanentný DoS stav

Spoločnosť Cisco opravila jednu kritickú (CVE-2018-15453) a jednu závažnú (CVE-2018-15460) chybu, ktoré dovoľujú v bezpečnostných produktoch pre e-mail spôsobiť permanentnú nedostupnosť služby jednoduchým odoslaním e-mailu. Obe chyby sa nachádzajú v Cisco AsyncOS softvéri pre Cisco Email Security Appliances. Prvá a súvisí s nevhodnou validáciou vstupu S/MIME podpísaných e-mailov. Druhá vychádza zo spôsobu, akým softvér filtruje e-maily s referenciami na whitelistované URL.

Juniper Networks opravila vyše 60 zraniteľností

Spoločnosť Juniper Networks opravila vyše 60 zraniteľností. V zariadeniach Juniper Advanced Threat Prevention to bolo 13 chýb spojených s natvrdo nakódovanými heslami, únikom informácií, XSS útokmi a vykonávaním ľubovoľných príkazov. 8 chýb bolo opravených v operačnom systéme Junos OS v knižnici na parsovanie XML dokumentov libxml2. Tieto chyby umožňujú okrem iného vykonávať DoS útoky. Dve zraniteľnosti súviseli s OpenSSL. V Junos Space bolo opravených takmer 40 zraniteľností. Jedna z nich označená ako kritická dovoľuje eskaláciu práv a vykonávanie ľubovoľného kódu. Väčšina ostatných je označená ako závažné.

36 ročné chyby v implementáciách SCP (PuTTY, OpenSSH, WinSCP)



Bezpečnostný výskumník Harry Sintonen informoval o štyroch zraniteľnostiach, ktoré objavil v protokole SCP. Škodlivému serveru dovoľujú meniť povolenia k cieľovej zložke u klienta, prepisovať ľubovoľné súbory a manipulovať s klientskym terminálom pomocou

ANSI kódu tak, aby sa ukryli nasledovné operácie. Zraniteľné sú všetky implementácie za posledných 36 rokov, teda aj PuTTY, OpenSSH a WinSCP. Vývojári aplikácií postupne vydávajú aktualizácie.

CMS Drupal malo dve kritické zraniteľnosti dovoľujúce vykonávať kód

Pre CMS Drupal 7, 8.5 a 8.6 vyšli aktualizácie na dve kritické chyby, ktoré umožňujú vykonávať kód. Jedna z nich dovoľuje vykonávať ľubovoľný PHP kód a súvisí so spôsobom, akým prúdový adaptér (wrapper) "phar://" narába s nedôveryhodnými URI. Druhá zraniteľnosť môže viesť k mazaniu súborov a vzdialenému vykonávaniu kódu. Súvisí s PHP knižnicou PEAR Archive_Tar na narábanie s .tar súbormi a zneužitá môže byť pomocou škodlivého .tar súboru cez prúdový adaptér "phar://".

Mesačník zraniteľností Január 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
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Správca softvérových balíčkov Linux APT
    - Windows Contacts

https://www.csirt.gov.sk/aktualne-7d7.html?id=176