MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Apríl 2021

Vypracoval: CSIRT.SK

TLP: White

V mesiaci apríl sa online platforma Codecov, určená na testovanie softvéru online, stala obeťou útoku. Platformu je možné integrovať do projektov na generovanie správ a štatistík ohľadom pokrytia kódu testami. Útočníci upravili skript Bash Uploader, pričom boli odhalené citlivé informácie zákazníckeho prostredia priebežnej integrácie (continuous integration – CI). Spoločnosť bola informovaná o kompromitácii 1. apríla 2021, avšak prvé náznaky útoku siahajú až do januára tohto roku. To znamená, že útok ostal nedetegovaný viac ako dva mesiace.

Codecov poskytuje nástroje, ktoré pomáhajú vývojárom merať, koľko zdrojového kódu sa počas testovania reálne vykoná (pokrytie kódu), čo slúži na odhalenie potenciálnych, predtým neodhalených chýb. Túto platformu využíva viac ako 29-tisíc spoločností medzi ktoré patrí Atlassian, Washington Post, GoDaddy a ďalšie.

Útočníkmi modifikovaný skript Bash Uploader je nástroj, ktorý zákazníci spoločnosti Codecov využívajú na zasielanie správ do platformy. Zisťuje špecifické nastavenia CI, zhromažďuje správy a nahráva informácie. Codecov sa o kompromitácii dozvedel od zákazníka, ktorý si všimol, že hash pre skript Bash Uploader na GitHube sa nezhoduje s hashom stiahnutého súboru.

Pár hodín po samotnom odhalení začal Codecov upozorňovať svojich zákazníkov, že sa stali obeťami útoku na dodávateľský reťazec. Bash Uploader využívajú tisícky firiem vo svojich projektoch. Upozornenie, ktoré zákazníci obdržali, hovorí o tom, že spoločnosť sa domnieva, že si útočníci stiahli repozitár.

Spoločnosť Codecov zverejnila indikátory kompromitácie, ktoré sú spojené s týmto útokom. Pôvodná IP adresa použitá na modifikáciu samotného skriptu je 79.135.72.34. Cieľové adresy, na ktoré sa prenášali údaje z napadnutého nástroja sú 178.62.86.114 a 104.248.94.23. Spoločnosť odhalila aj ďalšie indikátory, ktoré by mohli súvisieť s incidentom. Tento útok je porovnávaný s útokom na SolarWinds, pretože útočníci sa zamerali na automatizačný nástroj, ktorého zneužitím môžu ohroziť tisíce zákazníkov.

Prvotné vyšetrovanie odhalilo, že už od 31. januára 2021 dochádzalo k periodickým neoprávneným zmenám skriptu Bash Uploader, ktoré umožňovali útočníkom exfiltrovať informácie používateľov, ktoré majú uložené v prostrediach CI. Pomocou Codecov sa útočníci snažili dostať aj k iným spoločnostiam, ktoré poskytujú technologické služby, ako napríklad IBM, HPE (Hewlett Packard Enterprise) a podobne. Ovplyvnené boli tiež spoločnosti HashiCorp, Twilio a Monday.com. V rámci spoločnosti HashiCorp došlo k úniku súkromného PGP kľúča, ktorý spoločnosť využíva na podpisovanie hashov slúžiacich na validáciu produktov spoločnosti. Spoločnosť Twilio uviedla, že kompromitovaný BashUploader použila v rámci malého počtu projektov.

Zákazníkom spoločnosti Codecov sa odporúča resetovať prihlasovacie údaje a kľúče, ktoré by mohli byť v dôsledku tohto útoku kompromitované a vykonať tiež audit systémov na odhalenie prítomnosti akýchkoľvek znakov škodlivej činnosti.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci apríl riešil najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Jednotka analyzovala škodlivé prílohy série emailov spojených so sofistikovanou spear-phishingovou kampaňou na inštitúciu v jej konštituencii. Odhalená bola aj kompromitácia e-mailového účtu zamestnanca tejto organizácie, z ktorého následne útočníci odosielali phishingové správy.

Opäť sa objavilo niekoľko hlásení niekoľkých podvodných vishingových telefonátov s tematikou technickej podpory spoločnosti Microsoft.

CSIRT.SK prijal tiež hlásenie o ransomvérovom útoku na obec, ktorá prišla o server obsahujúci evidenciu obyvateľstva a účtovný systém. Dáta obec obnovila z marcovej zálohy, pričom stratila niekoľkotýždňové záznamy. Tieto bola schopná obnoviť z papierovej formy. Útočník použil ransomvér rodiny Phobos.

V médiách sa v mesiaci apríl objavila zmienka o prešovskej škole, kde neznámy útočník získal prístupové údaje ku kontu žiaka a rozposielal ostatným žiakom pornografický materiál. CSIRT.SK reagoval na túto správu a dožiadal si viac informácií. Nejednalo sa o závažnejší incident. So školou odkonzultoval ďalší postup pri jeho riešení.

Jednotka vykonala opakované testy zraniteľností do internetu vypublikovaných systémov niekoľkých zdravotníckych organizácií. Ich odstraňovanie riešila v spolupráci s SK-CERT NBÚ. Svoju konštituenciu varovala pred novými kritickými zraniteľnosťami serveru Microsoft Exchange a spísala odporúčania pre prevenciu a odpoveď na ransomvérové útoky, spolu s aktuálnymi vektormi, ktoré útočníci využívali najčastejšie.

Významné útoky vo svete

Infikovaná aplikácia WhatsApp Pink preberá kontrolu nad zariadením

Trójsky kôň s názvom #WhatsApp Pink bol rozšírený o funkcie, vďaka ktorým môže falošná aplikácia pre Android automaticky odpovedať na správy v aplikáciách Signal, Telegram, Viber a Skype. WhatsApp Pink označuje aplikáciu, ktorá obsahuje trójskeho koňa schopného prebrať kontrolu nad zariadením. Malvér sa šíri v skupinových konverzáciách v podobe správ „Apply New Pink Must Try New WhatsApp. http://XXXXXXXX/?whatsapp“. Odkaz smeruje na stránku, kde si používatelia môžu stiahnuť škodlivý APK súbor.

Indická služba na dodávanie potravín sa stala obeťou útoku

Na hackerskom fóre bolo zverejnených viac ako 20 miliónov záznamov používateľov služby dodávania potravín BigBasket. K narušeniu došlo už v novembri 2020, avšak skupina ShinyHunters sa rozhodla zverejniť databázu bezplatne až v apríli roku 2021. Databáza obsahuje emailové adresy, mená, hashované heslá, dátumy narodenia a telefónne čísla. Heslá sú hashované pomocou SHA1, pričom útočníci tvrdia, že sa im podarilo prelomiť už 2 milióny hesiel. Dôrazne sa odporúča, aby si všetci používatelia BigBasket okamžite zmenili svoje heslá.

V obchode Google Play sa vyskytuje škodlivá aplikácia FlixOnline tváriaca sa ako Netflix

V obchode Google Play bol nájdený nový červí mobilný malvér. Škodlivá aplikácia s názvom FlixOnline sa maskuje ako legitímna aplikácia Netflix. Podvodná aplikácia sľubovala neobmedzenú zábavu a dva mesiace prémiového predplatného v rámci Netflixu zadarmo kvôli pandémii. Po stiahnutí malvér odpočúva konverzácie v rámci aplikácie WhatsApp a odpovedá na prichádzajúce správy. Podľa výskumníkov sa malvér môže ďalej šíriť prostredníctvom škodlivých odkazov.

Škodlivé webové stránky sa snažia od používateľov získať informácie o kartách a prihlasovacie údaje.

Metropolitné policajné oddelenie utrpelo únik údajov o veľkosti 250 GB

Metropolitné policajné oddelenie (MPD), tiež známe ako DC Police, utrpelo útok ransomvérom Babuk. Útočníci zverejnili snímky ukradnutých súborov a priečinkov, pričom tvrdia, že dokopy vlastnia 250GB nezašifrovaných údajov. Zdá sa, že uniknuté údaje zahŕňajú súbory súvisiace s operáciami, disciplinárnymi záznamami a súbory, ktoré sa týkajú rôznych „gangov" a skupín pôsobiacich vo Washingtone DC. Útočníci varovali MPD, že majú 3 dni na to, aby ich kontaktovali, inak budú kontaktovať miestne skupiny, aby ich varovali pred policajnými informátormi.

Útočníci zneužívajú zraniteľné zariadenia spoločnosti QNAP

Vo svete sa šíri ransomvérová kampaň zameraná na zariadenia spoločnosti QNAP, pričom používatelia nachádzajú svoje súbory v archívoch 7zip, ktoré sú chránené heslom. Za týmito útokmi stojí ransomvér Qlocker. Súbory sú archivované v súboroch končiacich na .7z, pričom heslo k archívom pozná len útočník. Používatelia na svojich zariadeniach nachádzajú súbor „!!!READ_ME.txt", kde sú informácie o výkupnom. Útočníci žiadajú vo väčšine prípadoch 0,01 Bitcoinu, pričom po zaplatení sa používateľom zobrazí heslo pre odomknutie archívov. Skupina za túto kampaň zarobila 260-tisíc dolárov v priebehu piatich dní.

Severokórejská skupina vytvorila falošnú bezpečnostnú spoločnosť SecuriElite

Severokórejská skupina vytvorila falošnú bezpečnostnú firmu. Útočníkov prvýkrát spozorovala skupina pre analýzu hrozieb (TAG) spoločnosti Google v januári tohto roku. V tom čase útočníci zo Severnej Kórey vytvorili sieť falošných profilov naprieč sociálnymi sieťami vrátane Twitteru, Keybase a LinkedIn. V marci tohto roku skupina útočníkov vytvorila falošnú

spoločnosť s názvom SecuriElite. Spoločnosť SecuriElite tvrdí, že má sídlo v Turecku a ponúka služby penetračného testovania, hodnotenia zabezpečenia softvéru a kód zneužívajúci bezpečnostné zraniteľnosti. Útočníci sa vydávajú za profesionálov v oblasti bezpečnostného výskumu a náborárov pre firmy v oblasti kybernetickej bezpečnosti.

Zo sociálnej siete uniklo viac ako 533 miliónov telefónnych čísel

Zo sociálnej siete Facebook bolo zadarmo sprístupnených viac ako 533 miliónov telefónnych čísel a iných osobných údajov používateľov. Sprístupnené údaje zahŕňali telefónne číslo, ID používateľa, meno, pohlavie, polohu, stav, povolanie, dátum narodenia a emailové adresy. Predpokladá sa, že v roku 2019 bola zneužitá už opravená chyba vo funkcii „Pridať priateľa“, ktorá útočníkom umožnila získať prístup k telefónnym číslam. V rámci úniku boli zverejnené tiež čísla zakladateľov Facebooku Marka Zuckerberga, Chrisa Hughesa a Dustina Moskovitza. Spoločnosť Facebook uvádza, že zverejnené údaje sú z roku 2019.

Na zariadeniach spoločnosti Huawei sa vyskytujú aplikácie infikované malvérom Joker

Viac ako 500-tisíc používateľov zariadení spoločnosti Huawei si stiahlo aplikácie infikované malvérom Joker. Tento malvér registruje obete na prémiové mobilné služby. V obchode AppGallery bolo nájdených 10 zdanlivo neškodných aplikácií, ktoré obsahovali škodlivý kód. Infikované aplikácie požadovali prístup k upozorneniam, čo im umožnilo zachytiť potvrdzovacie kódy doručené prostredníctvom SMS. Medzi škodlivé aplikácie patrí Super Keyboard, Happy Colour, BeautyPlus Camera a podobne. Doctor Web informoval Huawei o týchto aplikáciách, pričom ich spoločnosť následne odstránila z AppGallery. Výskumníci tvrdia, že rovnaké moduly boli prítomné aj v iných aplikáciách v obchode Google Play, ktoré využívajú iné verzie malvéru Joker.

Spoločnosť Click Studios utrpela útok, ktorý súvisí s preposielaním údajov zo správcu hesiel Passwordstate

Spoločnosť Click Studios, ktorá stojí za vytvorením správcu hesiel Passwordstate, sa stala obeťou útoku. Podľa e-mailu obsahujúceho informácie ohľadom útoku, ktorý bol odoslaný zákazníkom, si zákazníci mohli medzi 20. a 22. aprílom stiahnuť škodlivé aktualizácie. Prvotná analýza poukazuje na to, že útočníci narušili funkcionalitu „In-Place Upgrade“. Po nasadení malvéru Moserpass sa zo zariadenia zhromažďujú informácie o systéme a údaje zo správcu hesiel Passwordstate. Následne sa tieto údaje preposielajú na servery kontrolované útočníkmi. Passwordstate využívajú používatelia rôznych spoločností po celom svete.

Útočníci opäť zaútočili na svojich „kolegov“ – hackerské fórum Swarmshop utrpelo únik

Kyberkriminálne fórum Swarmshop sa stalo obeťou útoku, pričom bola zverejnená databáza obsahujúca údaje o ukradnutých platobných kartách. Databáza obsahuje viac ako 600-tisíc záznamov o platobných kartách od vydavateľov kariet v Brazílii, Kanade, Číne, Francúzsku a podobne. Až 63% údajov sa týka obyvateľov USA. Databáza tiež obsahuje 498 súborov prihlasovacích údajov k online bankovníctvu. Tento útok je opäť dôkazom toho, že ani kriminálne fóra nie sú nedotknuteľné.

Zo sociálnej siete LinkedIn bolo zverejnených viac ako 500 miliónov údajov o používateľoch

Útočníci zverejnili osobné údaje o viac ako 500 miliónoch používateľov sociálnej siete LinkedIn, ktoré získali z verejných profilov. Archív zverejnených údajov obsahuje LinkedIn ID, celé mená, tituly, emailové adresy, telefónne čísla a ďalšie osobné údaje. Spoločnosť uvádza, že sa jedná o agregáciu údajov z mnohých webových stránok. Súkromné údaje nie sú súčasťou úniku. CyberNews zverejnil online nástroj, pomocou ktorého si používatelia môžu skontrolovať či sa stali obeťou úniku.

TLP: White

Spoločnosť DigitalOcean utrpela únik fakturačných údajov

Spoločnosť DigitalOcean sa stala obeťou útoku. Neoprávnený útočník pristúpil k rôznym fakturačným údajom z obdobia 9. apríl až 22. apríl 2021. Uniknuté údaje zahŕňajú meno zákazníka, fakturačnú adresu, dátum expirácie platobnej karty, posledné štvorčíslie kreditnej karty a názov banky. Spoločnosť uviedla, že chybu, ktorá toto narušenie spôsobila, už opravila. Viceprezident spoločnosti uviedol, že táto chyba odhalila iba 1% fakturačných profilov. DigitalOcean uvádza, že viac ako 1 milión vývojárov po celom svete využíva ich služby.

- **Malvér HackBoss kradne digitálne meny pomocou aplikácie Telegram.**
- **Únik BGP narušil tisícky sietí.**
- **Ransomvér Ryuk využíva nové techniky na získanie počiatočného prístupu do siete obete.**
- **NitroRansomware namiesto skutočných peňazí vyžaduje od obetí darčekové kódy Discord Nitro.**
- **Poskytovateľ poistenia pre automobily Geico utrpel únik údajov.**
- **Skupina Lazarus využíva BMP obrázky na skrytie malvéru RAT.**
- **Falošný Microsoft Store a stránky Spotify šíria malvér, ktorý kradne informácie.**
- **Bezpečnostní výskumníci odhalili v Google Play niekoľko podvodných aplikácií.**
- **Útočníci využívajú Telegram na riadenie malvéru ToxicEye.**
- **Útočníci sa pokúšajú zneužiť opravenú zraniteľnosť v produktoch Apex One, Apex One as a Service a OfficeScan.**
- **Ransomvér Mount Locker využíva vo svojich útokoch nové taktiky.**

- **Útočníci zneužívajú zraniteľnosti VPN na nasadenie malvéru Supernova na platformy SolarWinds Orion.**
- **Botnet aktívne skenuje zraniteľné servery Windows a Linux a infikuje ich malvérom na ťažbu kryptomeny Monero.**
- **Útočníci stojaci za ransomvérom REvil sa vyhrážajú, že zverejnia nové logá spoločnosti Apple.**
- **Trh s hudobnými nástrojmi Reverb utrpel únik údajov.**
- **FBI zdieľalo 4 milióny emailových adries, ktoré boli zozbierané malvérom Emotet.**
- **Hackerské fórum OGUsers bolo napadnuté už štvrtýkrát za dva roky.**
- **Brazílsky súdny systém Rio Grande do Sul zasiahol ransomvér REvil.**
- **Neznáma čínska APT skupina sa zameriava na ruský obranný sektor.**
- **Babuk ukončil šifrovanie ransomvérom, zameriava sa na vydieranie.**
- **Školský obvod na Floride bol zasiahnutý ransomvérom.**
- **Útočníci z Číny sa zameriavajú na vietnamskú armádu a vládu.**
- **Organizácie bojujúce proti COVID-19 čelili nárastu kybernetických útokov kvôli prechodu na cloudové platformy.**
- **Ruský útočník predal na hackerskom fóre takmer 900-tisíc darčekových kariet v celkovej hodnote odhadovanej na 38 miliónov dolárov.**
- **Indická maklérska spoločnosť Upstox utrpela únik 2,5 milióna údajov o používateľoch.**
- **Údaje 1,3 milióna používateľov aplikácie Clubhouse sú bezplatne vystavené na hackerskom fóre.**
- **Nový malvér pre Linux a macOS je skrytý vo falošnom npm balíčku s názvom „web-browserify“.**

Závažné zraniteľnosti bežných softvérových produktov

Nové kritické zraniteľnosti emailového serveru Microsoft Exchange

Národná bezpečnostná agentúra (NSA) informovala spoločnosť Microsoft o objave kritických zraniteľností umožňujúcich vzdialene vykonať kód (RCE) v produkte Microsoft Exchange Server. Spoločnosť Microsoft vydala bezpečnostné aktualizácie a apeluje na administrátorov, aby urgentne aktualizovali emailové servery Microsoft Exchange vo svojej správe. Aktuálne nebolo zaznamenané zneužitie týchto zraniteľností, avšak Microsoft predpokladá, že je to len otázkou času.

BleedingTooth – zraniteľnosti bluetooth v systéme Linux teraz už aj s exploitom

BleedingTooth je sada zraniteľností zariadení Bluetooth v operačnom systéme Linux. Zraniteľnosti umožňujú útočníkovi bez interakcie obete napadnúť zariadenia s oprávneniami jadra systému. Tieto staršie zraniteľnosti predstavujú stále riziko pre veľký počet neaktualizovaných zariadení po celom svete. Ešte väčšiu váhu im dáva aktuálne dostupná ukážka zneužitia zraniteľnosti (PoC exploit).

Spoločnosť Cisco neopraví kritické zraniteľnosti svojich produktov

Spoločnosť Cisco sa rozhodla neopraviť kritické zraniteľnosti niektorých svojich smerovačov a zariadení firewall, ktorým skončila softvérová podpora. Spoločnosť Cisco vyzýva spoločnosti, ktoré tieto zariadenia používajú, aby zariadenia vymenili za novšie, podporované.

Spoločnosť Cisco opravila kritickú zraniteľnosť produktu SD-WAN vManage

Spoločnosť Cisco vydala aktualizácie na opravu zraniteľností. Jedna zraniteľnosť získala hodnotenie „kritická“. Spoločnosť Cisco apeluje na administrátorov k čo najrýchlejšej oprave zariadení v ich správe.

Stará zraniteľnosť firewallov od Spoločnosti Fortinet je aktívne zneužívaná

Stará zraniteľnosť firewallov Fortinet SSL VPN z roku 2018 je aktuálne aktívne zneužívaná. Okrem priamych zneužití zraniteľností, začali zraniteľnosť CVE-2018-13379 útočníci zneužívať aj na šírenie ransomvéru (napríklad ransomvér Cring). Rovnako s rozšírením povedomia o zneužiteľnosti zraniteľnosti a s poznatkom, že existuje množstvo zariadení, ktoré neboli administrátormi opravené, bolo pozorované aj masívne skenovanie sietí vyhľadávajúc zraniteľné zariadenia na ktoré by mohli útočníci potencionálne útočiť.

V Pulse Connect Secure (PCS) SSL VPN bola opravená kritická aktívne zneužívaná zero-day zraniteľnosť

V Pulse Connect Secure (PCS) SSL VPN bola objavená a opravená aktívne zneužívaná zero-day zraniteľnosť, ktorej zneužitím môže dôjsť k vzdialenému vykonaniu kódu neautentifikovaným útočníkom. Zraniteľnosť dosahuje CVSS skóre 10.

Spoločnosť SonicWall opravila kritické zraniteľnosti produktu pre emailovú bezpečnosť

Spoločnosť SonicWall opravila 3 vážne zraniteľnosti, ktoré získali hodnotenie CVSS 6,7 a 9,4. Najzávažnejšia zo zraniteľností by mohla útočníkovi umožniť vzdialene vytvoriť administrátorský účet poslaním špeciálne vytvorenej http požiadavky zraniteľnému zariadeniu. CSIRT.SK odporúča bezodkladne aktualizovať zraniteľné zariadenia vo svojej správe a predísť tak odcudzeniu dát, či možnému rozšíreniu malvéru v organizácii.

Mesačník zraniteľností Apríl 2021

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
    - Nové kritické zraniteľnosti emailového serveru Microsoft Exchange
    - BleedingTooth – zraniteľnosti bluetooth v systéme Linux teraz už aj s exploitom
    - Spoločnosť Cisco neopraví kritické zraniteľnosti svojich produktov
    - Spoločnosť Cisco opravila kritickú zraniteľnosť produktu SD-WAN vManage
    - Stará zraniteľnosť firewallov od Spoločnosti Fortinet je aktívne zneužívaná
    - V Pulse Connect Secure (PCS) SSL VPN bola opravená kritická aktívne zneužívaná zero-day zraniteľnosť
    - Spoločnosť SonicWall opravila kritické zraniteľnosti produktu pre emailovú bezpečnosť

https://www.csirt.gov.sk/aktualne-7d7.html@id=243