MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2021

Vypracoval: CSIRT.SK

TLP: White

Začiatkom mesiaca marec boli objavené 4 aktívne zneužívané zero-day zraniteľnosti v serveroch Microsoft Exchange, ktoré bližšie popisujeme na našej stránke. Spôsobili značné problémy správcom serverov Exchange po celom svete. Kvôli týmto zraniteľnostiam boli útočníci schopní získať prístup k emailovým účtom a tiež nainštalovať dodatočný malvér na zariadenia s cieľom získať dlhodobý prístup do systémov obete. Microsoft Threat Intelligence Center (MSTIC) pripisuje túto kampaň s najväčšou pravdepodobnosťou skupine Hafnium.

Skupina Hafnium je pravdepodobne štátom sponzorovaná čínska skupina pôsobiaca mimo Čínu. Primárne sa zameriava na subjekty v USA v mnohých odvetviach. Vo svojich útokoch nevynecháva právnické firmy, vzdelávacie inštitúcie a podobne.

V pozorovaných kampaniach boli tieto 4 chyby zneužité na získanie počiatočného prístupu k cieľovým serverom Exchange a na dosiahnutie vzdialeného vykonania kódu. Útočníci zo skupiny Hafnium následne na kompromitované servery nasadili webové shelly (príkazové riadky), ktoré neskôr použili na krádež dát a rozšírenie útoku.

Neskôr sa ukázalo, že spomínané zraniteľnosti zneužívajú aj iné skupiny, pričom boli identifikované útoky na servery nielen v USA, ale aj v Európe, Ázii a na Blízkom východe. Útoky boli zamerané na vládne organizácie, právnické firmy, zdravotnícke zariadenia a súkromné spoločnosti. Prvotná analýza približne 2000 Exchange serverov odhalila, že zhruba 400 z nich bolo zraniteľných a ďalších 100 potenciálne zraniteľných.

Zraniteľnosti boli opravené v najnovších aktualizáciách, avšak ukázalo sa, že nie pre každý server sú tieto aktualizácie aplikovateľné. Preto spoločnosť Microsoft vydala alternatívne zmierňujúce opatrenia, ktoré však nie sú náhradou za nápravu, a tiež nepredstavujú úplnú ochranu pred útokmi.

Taktiež bola vydaná nová aktualizácia nástroja Microsoft Safety Scanner (MSERT), ktorý je schopný detegovať webové shelly. Spoločnosť vydala aj skript, ktorý je schopný skontrolovať na zariadení indikátory kompromitácie. Ďalej boli vydané dodatočné aktualizácie ProxyLogon pre verzie tých Exchange serverov, ktoré nepodporujú pôvodné bezpečnostné aktualizácie. Sú dostupné len cez Microsoft Download Center.

Každým dňom závažnosť zneužívania týchto zraniteľností rástla. Zamerali sa na ne tiež operátori ransomvéru, pričom celkový počet útokov exponenciálne narástol iba v priebehu niekoľkých dní. Rodina ransomvérov použitá pri útokoch sa označuje aj ako DearCry. Spoločnosť Eset odhalila minimálne 10 rôznych zločineckých skupín, ktoré tieto zraniteľnosti zneužívali. Jedná sa konkrétne napríklad o Calypso, LuckyMouse (APT27), Winnti Group (APT41) a ďalšie.

Spoločnosť Microsoft odhalila, že k 12. marcu zostávalo ešte aktualizovať viac ako 82 000 Exchange serverov (zo 400 000 identifikovaných 1. marca). Tiež zdôraznila, že prvým krokom na ochranu serverov je použitie dostupných opráv. Následne je potrebné identifikovať ohrozené systémy a odstrániť ich zo siete.

Ukázalo sa, že medzera medzi vydaním aktualizácií a reálnym aktualizovaním systémov bola dostatočne veľká na to, aby útočníci tieto zraniteľnosti začali vo veľkom aktívne zneužívať. Preto je vysoko odporúčané riadiť sa radami, ktoré vydala spoločnosť Microsoft, aby tak organizácie po prvé predišli prípadnej kompromitácii serverov, a po druhé aby už zrealizovanú kompromitáciu odhalili.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci marec riešil najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Jednou z vážnejších hrozieb bola phishingová kampaň imitujúca identitu Finančnej správy SR, ktorá mala za cieľ odcudziť osobné údaje obete a informácie o jej platobnej karte. Viac informácií o podvodných emailoch môžete nájsť na stránkach Finančnej správy, informácie o mechanizme fungovania útoku zas na stránkach NBÚ.

Mesiacu marec dominovala séria kritických zraniteľností mailserverov Microsoft Exchange. Jednalo sa o zraniteľnosti typu zero-day, teda informácie o nich boli dostupné útočníkom už pred ich opravou. Spoločnosť Microsoft detegovala ich aktívne zneužívanie v kampani, ktorú pripísala čínskej APT skupine Hafnium. CSIRT.SK bezodkladne varoval svoju konštituenciu. Následne začal kampaň na odhalenie a opravu zraniteľných serverov organizácií vo svojej konštituencii. Odhalil tiež viacero zraniteľných slovenských organizácií mimo svojej konštituencie. O nálezoch informoval Národnú jednotku SK-CERT (NBÚ). V rámci kampane bolo identifikovaných niekoľko kompromitovaných zariadení. V týchto prípadoch jednotka vykonala potrebné činnosti na zistenie dopadov a zabezpečenie mailserverov, vrátane vedenia vyšetrovania, alebo asistencie pri riešení incidentov. Všetky zaznamenané kompromitácie sa javili ako prípravná fáza komplexného útoku a neboli zaznamenané úniky údajov. CSIRT.SK dohliadol na to, aby všetky odhalené zraniteľné servery MS Exchange v jeho konštituencii prešli potrebnou aktualizáciou.

Vládna jednotka CSIRT sa potýkala s phishingovou kampaňou cielenou na inštitúciu vo svojej konštituencii, na ktorú smerovala séria podvodných emailov. Tieto boli pomerne dôveryhodne sformulované a obsahovali prílohy, ktoré predstierali dokumenty známe zamestnancom danej inštitúcie. Prevažne obsahovali nástroje, vďaka ktorým by interakcia s dokumentom viedla ku kompromitácii zariadenia obete.

CSIRT.SK riešil tento mesiac tiež prípad ransomvéru v strednej škole, ktorá prišla o dáta z niekoľkých serverov, vrátane záloh. Jednalo sa o variant ransomvéru Phobos.

Pri analýze inej vzorky malvéru sa analytici jednotky dostali ku zoznamu kompromitovaných IP adries, ktorý si útočníci generovali automaticky na doméne uvedenej v zdrojovom kóde. CSIRT.SK informoval národné jednotky CSIRT štátov, ktorých IP adresy sa v zozname vyskytli.

Vládna jednotka riešila únik citlivých údajov cez internetovú službu Uloz.to, odkiaľ boli predmetné súbory nakoniec vymazané. Vyšetrovala tiež podozrenie na prienik na portál korona.gov.sk, kde sa

v zdrojovom kóde objavil ASCII art zobrazujúci družicu Sputnik. Prienik sa nepotvrdil a jednalo sa len o recesiu vývojárov.

CSIRT.SK varoval svoju konštituenciu aj pred zero-day zraniteľnosťou prehliadača Google Chrome. Ďalšie tri komunikované zraniteľnosti v systémoch Windows a Windows Server boli opravené v rámci pravidelného balíka aktualizácií Patch Tuesday. Odhalené boli v prehliadačoch Internet Explorer a Edge, DNS serveri a v službe Win32K. Posledné varovanie súviselo s aktívne zneužívanou kritickou zraniteľnosťou sieťových zariadení F5 BIG-IP a BIG-IQ.

Významné útoky vo svete

Útočníci narušili servery spoločnosti SITA

Údaje o cestujúcich viacerých leteckých spoločností unikli po tom, čo útočníci narušili servery patriace spoločnosti SITA, ktorá poskytuje informačné technológie. Celkový počet dotknutých osôb nie je známy, avšak určite presiahol hodnotu 2,1 milióna. Únik zasiahol spoločnosti Lufthansa, Air New Zealand, Singapore Airlines, SAS, Cathay Pacific, Jeju Air, Malaysia Airlines a Finnair. Viacero spoločností už kontaktovalo svojich zákazníkov, aby ich informovali o možnom úniku ich údajov.

Spoločnosť Sierra Wireless čelila útoku ransomvérom

Spoločnosť Sierra Wireless sa stala obeťou útoku ransomvérom. Útok zasiahol vnútornú sieť spoločnosti. Spoločnosť tvrdí, že nemal dopad na žiadne služby ani produkty zamerané na zákazníkov. Po útoku bola spoločnosť nútená odstaviť výrobné závody na celom svete. Narušená bola aj webová stránka spoločnosti a ďalšie interné operácie. Spoločnosť neposkytla žiadne informácie o tom, aký ransomvér stál za útokom, a tiež či pred samotným šifrovaním boli ukradnuté dokumenty z kompromitovaných systémov.

Malvér Purple Fox má nový červí modul, ktorý je schopný infikovať systémy Windows

Donedávna sa malvér Purple Fox distribuoval prostredníctvom exploitových súprav a phishingových emailov. Avšak neskôr bol pridaný červí modul, ktorý mu umožňuje počas prebiehajúceho útoku vyhľadávať a infikovať systémy Windows dosiahnuteľné cez internet. Zatiaľ čo nové správanie Purple Fox podobné červom umožňuje infikovať servery prostredníctvom služieb SMB, na nasadenie škodlivého kódu tiež využíva phishingové kampane a chyby webového prehliadača.

Z Play Store bolo odstránených 10 aplikácií, ktoré obsahovali program na prenos trójskych koní

Google z obchodu Play Store odstránil 10 aplikácií, ktoré obsahovali program na prenos trójskych koní. Medzi tieto aplikácie patria Cake VPN, Pacific VPN, BeatPlayer, QR/Barcode Scanner MAX a QRecorder. Novoobjavený škodlivý program bol nazvaný Clast82. Bol navrhnutý pre doručenie malvéru zameraného na finančnú trestnú činnosť. Po spustení sa z GitHubu stiahne škodlivý kód mRAT a AlienBot. MRAT slúži na zabezpečenie vzdialeného prístupu k napadnutému mobilnému zariadeniu, zatiaľ čo AlienBot uľahčuje vkladanie škodlivého kódu do existujúcich legitímnych finančných aplikácií.

Oficiálny Git repozitár PHP bol napadnutý útočníkmi

V marci bol napadnutý oficiálny Git repozitár PHP. Útočníci neoprávnene manipulovali s kódovou základňou. V úložisku php-src na serveri git.php.net boli vykonané 2 škodlivé zmeny. Útočníci sa však podpísali ako známi vývojári a správcovia PHP. Do kódu nasadili zadné vrátka, ktoré umožňujú vzdialené vykonávanie kódu. Ako preventívne opatrenie po tejto udalosti sa správcovia PHP rozhodli migrovať oficiálne úložisko zdrojových kódov PHP na GitHub. Incident je vnímaný ako závažný vzhľadom k tomu, že 79% webových stránok na internete využíva práve programovací jazyk PHP.

Nový malvér RedXOR sa zameriava na operačný systém Linux

Čínski útočníci používajú pri svojich útokoch nový malvér s názvom RedXOR. Maskuje sa ako polkitový démon. Útoky sú zamerané na systémy s operačným systémom Linux. Názov RedXOR súvisí so skutočnosťou, že kóduje sieťové údaje pomocou schémy založenej na XOR a je kompilovaný so starým kompilátorom GCC na starom vydaní Red Hat Enterprise Linux. Vzorky tohto malvéru boli nahrané na VirusTotal z Taiwanu a Indonézie. RedXOR prichádza s rozsiahlou sadou

funkcií. Dokáže napríklad vykonávať príkazy so systémovými oprávneniami, skrývať svoj vlastný proces pomocou open-source rootkitu Adore-ng, či prenášať škodlivé údaje cez proxy a podobne.

Spoločnosť Oxfam Australia utrpela únik údajov o veľkosti 1,7 milióna záznamov

Spoločnosť Oxfam Australia sa stala obeťou kybernetického útoku, pričom odcudzené boli údaje z databázy darcov. Oxfam Australia je charitatívna organizácia zameraná na zmierňovanie chudoby v Afrike, Ázii a na Blízkom východe. Databáza, ktorá sa vyskytla na hackerskom fóre, obsahuje až 1,7 milióna záznamov o používateľoch. Záznamy zahŕňajú mená, emailové adresy, adresy bydliska, telefónne čísla a sumy, ktoré darovali spoločnosti. Databáza obsahuje informácie o podporovateľoch, ktorí podpísali petíciu, zúčastnili sa kampane alebo poskytli dary a podobne. Nedošlo však ku zneužitiu hesiel.

Hackerské fórum Maza bolo napadnuté útočníkmi

Hackerské fórum Maza napadli útočníci, pričom unikli údaje o približne 2982 členoch. Uniknuté údaje zahŕňajú ID používateľa, používateľské meno, emailovú adresu, heslá, názvy súborov certifikátov, heslá pre certifikáty, kontaktné informácie a podobne. Samotné certifikáty neboli odhalené. Takéto útoky dokazujú, že nikto nie je v bezpečí pred kybernetickými útokmi, vrátane samotných útočníkov. Ukázalo sa, že Maza nie je jediným hackerským fórom, ktoré sa stalo terčom útokov. Medzi napadnuté fóra patria aj Verified, Dread a Club2Crd.

Malvér CopperStealer zhromažďuje heslá uložené vo webových prehliadačoch

Nový malvér označený ako CopperStealer sa zameriava na používateľov hlavných poskytovateľov služieb ako Google, Facebook, Amazon a Apple. Útočníci stojaci za týmto malvérom vo svojich kampaniach použili kompromitované účty na spustenie škodlivých reklám

a na dodanie ďalšieho škodlivého softvéru. CopperStealer funguje na princípe zhromažďovania hesiel uložených vo webových prehliadačoch Chrome, Edge, Firefox, Yandex a Opera. Je schopný získať prístupový token pre Facebook pomocou ukradnutých cookies. CopperStealer sa distribuuje prostredníctvom falošných stránok ako napríklad keygenninja[.]com, piratewares[.]com a podobne.

Spoločnosť Molson Coors bola kvôli útoku ransomvérom nútená pozastaviť obchodné operácie

Spoločnosť Molson Coors, ktorá je známa vďaka značkám piva ako Coors Light, Miller Lite, Molson Canadian a podobne, utrpela útok ransomvérom. Tento útok spôsobil výrazné narušenie činnosti spoločnosti vrátane výroby a prepravy piva. Útok mal za následok, že spoločnosť vypla svoje systémy, aby zabránila ďalšiemu šíreniu ransomvéru. Z dôvodu, že zamestnanci nemajú prístup k špecifickým systémom, došlo k narušeniu obchodných operácií. Nie je známe, či bol útok smerovaný do podnikovej siete Molson Coors, alebo či sa rozšíril do sietí značiek tejto spoločnosti.

Výskumníci odhalili ďalšie 3 kmene škodlivého softvéru v súvislosti s útokmi na Solarwinds

Bezpečnostní výskumníci v spolupráci s Microsoft Threat Intelligence Center (MSTIC) a Microsoft 365 Defender Research Team našli tri nové kmene škodlivého softvéru s názvom GoldMax, Sibot a GoldFinder v súvislosti s útokmi na SolarWinds. Tieto kmene boli využité na udržanie perzistencie a vykonávanie akcií v sieťach po kompromitácii, pričom sa dokázali vyhnúť prvotnej detekcii. GoldMax je malvér písaný v jazyku Go, ktorý útočníci použili na ukrytie škodlivej činnosti a vyhnutie sa detekcii. Sibot je malvér založený na VBScript, pričom sa využíval na udržanie perzistencie a stiahnutie ďalších častí škodlivého softvéru. GoldFinder je tiež založený na jazyku Go a bol pravdepodobne využívaný ako vlastný sledovací nástroj.

Útočníci získali prístup ku 150-tisíc kamerám spoločnosti Verkada

Útočníci získali prístup k 150-tisíc živým kamerám spoločnosti Verkada. Spomínané kamery sa nachádzajú v spoločnostiach Tesla, Equinox, zdravotníckych klinikách, väzniciach a bankách. Podľa reverzného inžiniera skupiny hackerov Tillie Kottmanna získali prístup k týmto monitorovacím systémom pomocou účtu superadministrátora pre spoločnosť Verkada, ktorá spolupracuje so spomenutými organizáciami. Kottman uviedol, že v exponovanej DevOps infraštruktúre našli pevne zadané prihlasovacie údaje. Po kontaktovaní spoločnosti Verkada útočníci stratili prístup k napadnutému účtu. Spoločnosť Verkada deaktivovala všetky účty interných správcov, aby tak zabránila neoprávnenému prístupu.

- Spoločnosť CompuCom MSP bola zasiahnutá ransomvérom DarkSide.
- 15 škôl vo Veľkej Británii nebolo schopných poskytovať online výučbu z dôvodu kybernetického útoku.
- Tisíce mobilných aplikácií vystavujú údaje prostredníctvom nesprávne nakonfigurovaných cloudových kontajnerov.
- Ransomvér Hog dešifruje zariadenia užívateľov iba v prípade, že sa pripoja k vývojárskemu serveru na Discord.
- Nový útok postranným kanálom sa zameriava na vzájomné prepojenie procesorov Intel s cieľom zhromaždiť citlivé údaje.
- Iránski útočníci využívajú softvér na vzdialené sledovanie svojich potenciálnych obetí.
- Banka Flagstar sa stala obeťou útoku ransomvéru Clop.
- Kampaň na ťažbu kryptomien zasiahla neopravené NAS zariadenia spoločnosti QNAP.
- Nový ransomvér Sabrloh šifruje súbory a súčasne prináša správu podporujúcu protesty indických farmárov.
- Už tretia francúzska nemocnica bola zasiahnutá ransomvérom.
- Spoločnosť Lactalis utrpela útok, kde tretia strana získala prístup do siete.
- Trójsky kôň Ursnif sa zameral na viac ako 100 talianskych bánk.
- Útočníci zdieľajú metódy, ako obísť 3D Secure pre platobné karty.
- Bezpečnostní výskumníci objavili malvér napísaný v programovacom jazyku Nim.
- Malvér XCSSET pre Mac bol prispôsobený pre zariadenia s čipmi M1.
- FBI varuje pred eskalovaním útokov ransomvéru Pysa na vzdelávacie organizácie.
- Shell je ďalšou obeťou útokov na produkt FTA spoločnosti Accellion.

- **Ransomvér REvil má nový šifrovací režim „Windows Safe Mode“.**
- **FBI varuje pred útokmi BEC, ktoré sa čoraz viac zameriavajú na americké vládne organizácie.**
- **Falošná verzia aplikácie Clubhouse šíri malvér BlackRock, ktorý kradne údaje zo 458 služieb.**
- **Spoločnosť Solairus Aviation utrpela únik údajov.**
- **Nemecký parlament je opäť terčom útokov ruských štátnych hackerov.**
- **Trójsky kôň Metamorfo Banking zneužíva AutoHotKey, aby zabránil detekcii.**
- **Stopy malvéru Supernova spájajú čínsku skupinu Spiral s útokmi na servery SolarWinds.**
- **Ázijská distribúcia potravín JFC International sa stala obeťou útoku ransomvéru.**
- **FINRA varuje pred prebiehajúcimi phishingovými útokmi zameranými na sprostredkovateľské firmy.**
- **Útočníci zo skupiny FIN8 sa vracajú s výkonnejšou verziou malvéru BADHATCH PoS.**

Závažné zraniteľnosti bežných softvérových produktov

Bola opravená kritická zraniteľnosť v prehliadači Chrome

Spoločnosť Google opravila aktívne zneužívanú kritickú zraniteľnosť nachádzajúcu sa v produkte Chrome. Verzia 89.0.4389 obsahujúca 47 opráv zraniteľností bola zverejnená 2. marca pre operačné systémy Windows, macOS a Linux. Najvážnejšia z nich sa týkala problému cyklu objektu vo zvuku.

Spoločnosť VMware opravila kritické zraniteľnosti vo svojich produktoch

Zraniteľnosti sa nachádzajú v systémoch ESXi, vCenter a ich doplnkoch. Týkajú sa všetkých základných inštalácií zraniteľných systémov. Ich úspešným zneužitím môže útočník získať schopnosť vzdialene vykonávať kód a získavať citlivé informácie zo sieťovej infraštruktúry, v ktorej je zraniteľné zariadenie pripojené. VMware odporúča čo najrýchlejšiu aktualizáciu na najnovšie verzie, avšak ak to nie je možné, spoločnosť prišla aj s dočasným riešením zraniteľností na nevyhnutný čas.

Kritická zraniteľnosť grafického prvku systému Windows 10

Dominik Röttsches z Google a Mateusz Jurczyk z Google Project Zero odhalili v novembri kritickú zraniteľnosť API rozhrania systému Windows, ktorá bola opravená spoločnosťou Microsoft vo Februárových bezpečnostných aktualizáciách systému. Chyba umožňuje vzdialene vykonávať kód.

Spoločnosť Cisco opravila 3 kritické zraniteľnosti v rôznych produktoch

Spoločnosť Cisco opravila 3 kritické zraniteľnosti, pričom jedna z nich dosahuje CVSS skóre 10. Táto zraniteľnosť sa nachádza v softvéri ACI Multi-Site Orchestrator. Súvisí s nesprávnou validáciou tokenu v koncovom bode API. Ďalšia chyba sa nachádza v operačnom systéme NX-OS v prepínačoch Nexus. Vzdialený

útočník vie manipulovať so súbormi bez akejkoľvek autentifikácie. Posledné zraniteľnosti ovplyvňujú Cisco Application Services Engine. Súvisia s nedostatočnou kontrolou prístupu k službe bežiacej v dátovej sieti.

Spoločnosť Microsoft v rámci balíka opráv Patch Tuesday opravila 89 zraniteľností

Spoločnosť Microsoft v rámci balíka opráv Patch Tuesday vydala opravu pre 89 zraniteľností, z čoho 14 je kritických a 75 závažných. Oprava sa týkala aj 2 zero-day zraniteľností, pričom jedna z nich (CVE-2021-26411 v prehliadačoch Internet Explorer a Edge) je aktívne zneužívaná. Zneužitím týchto zraniteľností môže dôjsť k vzdialenému vykonávaniu kódu, poškodeniu pamäte a eskalácií privilégií.

V produktoch spoločnosti SAP sa nachádzajú 2 kritické zraniteľnosti

Spoločnosť SAP v rámci marcových bezpečnostných aktualizácií opravila 2 kritické zraniteľnosti. Nachádzajú sa v aplikáciách SAP MII a SAP NetWeaver AS Java. Chyby môžu viesť k vzdialenému vykonávaniu kódu a tiež k úplnej kompromitácii zraniteľného systému.

Závažná zraniteľnosť v zariadeniach od spoločnosti Apple

Spoločnosť Apple vydala opravu zraniteľnosti CVE-2021-1844, ktorá môže viesť ku vzdialenému vykonávaniu kódu. Chyba sa týka zariadení so systémom iOS, macOS, watchOS a webového prehliadača Safari. Vyskytuje sa vo frameworku WebKit. Používateľom je odporúčané nainštalovať si najnovšie dostupné aktualizácie.

Ďalšia aktívne zneužívaná zero-day zraniteľnosť v prehliadači Chrome

V prehliadači Chrome spoločnosti Google bola opravená ďalšia aktívne zneužívaná zero-day zraniteľnosť. Súvisí s použitím odalokovaného miesta v pamäti v nástroji Blink. Úspešným zneužitím môže dôjsť k vzdialenému vykonávaniu kódu alebo k narušeniu dostupnosti systému.

Spoločnosť F5 varuje pred kritickými zraniteľnosťami svojich produktov

Spoločnosť F5 vydala bezpečnostné aktualizácie svojich produktov, ktoré opravujú kritické zraniteľnosti. Zraniteľnosti by mohli byť zneužité na vzdialené vykonanie kódu (RCE), alebo spôsobenie nedostupnosti služby (DoS). S veľkou váhou apeluje na administrátorov aj organizácia CISA, ktorá upozorňuje na potrebu zabezpečenia produktov spoločnosti F5 pre zamedzenie zneužívania kritických zraniteľností.

Aktívne zneužívaná kritická zraniteľnosť produktov SonicWall

V produktoch SonicWall Secure Mobile Access 100 (SMA 100) sa nachádza zraniteľnosť typu SQL injection, ktorej zneužitie môže viesť ku neoprávnenému prihláseniu do zariadenia. Produkty SMA 100 sa používajú na vzdialený prístup. Viacero bezpečnostných autorít reportovalo, že je zraniteľnosť aktívne zneužívaná. Z toho dôvodu je potrebné produkty bezodkladne aktualizovať.

Zraniteľnosti v jadre systému Linux objavené po 15 rokoch

Kyberbezpečnostná spoločnosť GRIMM zverejnila trojicu chýb, ktorú objavila v jadre operačného systému Linux. Zraniteľnosti sa nachádzajú v nepovšimnutom kóde, kde čakali celých 15 rokov. Útočníkom umožňujú eskalovať privilégiá, odcudziť informácie, či spôsobiť nedostupnosť služby.

V produkte Cisco Jabber bolo opravených 5 zraniteľností

Spoločnosť Cisco vydala záplatu pre 5 zraniteľností vyskytujúcich sa v produkte Cisco Jabber pre Windows, MacOS a mobilné platformy. Kritická zraniteľnosť je spôsobená nesprávnym overovaním obsahu XMPP správy, čo môže viesť ku vzdialenému vykonávaniu kódu. Zneužitím zvyšných 4 chýb môže dôjsť tiež ku vzdialenému vykonaniu kódu, úniku citlivých informácií alebo narušeniu dostupnosti služby.

V klientskom softvéri Zoom sa vyskytuje chyba, ktorá môže viesť k odhaleniu citlivých informácií

Vo videokonferenčnej platforme Zoom sa nachádza zraniteľnosť pri zdieľaní obrazovky, ktorej zneužitím môže dôjsť k vyzradeniu citlivých informácií. Chyba zatiaľ nie je opravená, avšak spoločnosť si je vedomá tohto problému a pracuje na jeho vyriešení.

Kritická zraniteľnosť v knižnici sieťovej masky, npm balíčku Netmask

Victor Viale, Sick Codes, Nick Sahler, Kelly Kaoundis a John Jackson informovali o kritickej zraniteľnosti npm knižnice masky siete, ktorá môže umožniť útočníkovi obísť určité mechanizmy ochrany siete a následne na ňu vykonať útoky. Knižnica npm netmask je využívaná po celom svete a má na konte stovky miliónov stiahnutí.

Spoločnosť Adobe opravila kritickú zraniteľnosť produktu ColdFusion

Spoločnosť Adobe vydala neplánované bezpečnostné aktualizácie pre produkt ColdFusion verzie 2016, 2018 a 2021. Zraniteľnosť by útočník mohol zneužiť na vzdialené vykonanie ľubovoľného kódu.

Projekt OpenSSL vydal opravu zraniteľností pre svoju knižnicu zabezpečujúcu šifrovanú komunikáciu

Projekt OpenSSL vydal opravu chýb pre svoju knižnicu, ktorú využívajú mnohé aplikácie a servery na zabezpečenie dôvernej komunikácie. Objavené zraniteľnosti môže útočník zneužiť na spôsobenie nedostupnosti služby, alebo ohroziť dôvernosť a integritu prenášaných dát šifrovaných protokolom TLS.

Mesačník zraniteľností Marec 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
    - Bola opravená kritická zraniteľnosť v prehliadači Chrome
    - Spoločnosť VMware opravila kritické zraniteľnosti vo svojich produktoch
    - Kritická zraniteľnosť grafického prvku systému Windows 10
    - Spoločnosť Cisco opravila 3 kritické zraniteľnosti v rôznych produktoch
    - Spoločnosť Microsoft v rámci balíka opráv Patch Tuesday opravila 89 zraniteľností
    - V produktoch spoločnosti SAP sa nachádzajú 2 kritické zraniteľnosti
    - Závažná zraniteľnosť v zariadeniach od spoločnosti Apple
    - Ďalšia aktívne zneužívaná zero-day zraniteľnosť v prehliadači Chrome
    - Spoločnosť F5 varuje pred kritickými zraniteľnosťami svojich produktov
    - Aktívne zneužívaná kritická zraniteľnosť produktov SonicWall
    - Zraniteľnosti v jadre systému Linux objavené po 15 rokoch
    - V produkte Cisco Jabber bolo opravených 5 zraniteľností
    - V klientskom softvéri Zoom sa vyskytuje chyba, ktorá môže viesť k odhaleniu citlivých informácií
    - Kritická zraniteľnosť v knižnici sieťovej masky, npm balíčku Netmask
    - Spoločnosť Adobe opravila kritickú zraniteľnosť produktu ColdFusion
    - Projekt OpenSSL vydal opravu zraniteľností pre svoju knižnicu zabezpečujúcu šifrovanú komunikáciu

https://www.csirt.gov.sk/aktualne-7d7.html?id=241