MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK
Apríl 2024

Vypracoval: CSIRT.SK

TLP: White

Kybernetickým priestorom v apríli 2024 rezonovalo hneď niekoľko tém súvisiacich s **útokmi na sieťové zariadenia** od rôznych výrobcov a **prípad dešifrovania** systémov **zasiahnutých ransomvérom po zaplatení výkupného**.

Útoky na sieťové zariadenia vzdialeného prístupu a perimetrovej ochrany, ako sú **VPN koncentrátory a firewally**, majú pre útočníka kľúčový význam z pohľadu ďalšieho prieniku do interných systémov. **V prípade** ich **úspešnej kompromitácie útočník získava** v rôznom rozsahu **prístup k internej sieťovej komunikácii**, **systémom a citlivým údajom a taktiež schopnosť efektívneho maskovania svojej činnosti**. Útoky na sieťové zariadenia zachytené v mesiaci apríl možno rozdeliť do dvoch veľkých častí.

Prvá časť útokov na sieťové zariadenia spočívala v **zneužití citlivých údajov odcudzených v rámci predchádzajúcich kybernetických útokov**. Ako konkrétne príklady možno použiť rozsiahle **password-spraying** a **brute-force** **kampane cielené na** služby **VPN** a **SSH**, na ktoré **upozornila spoločnosť CISCO**. Pri **password-spraying** útoku sa **útočník pokúša o prihlásenie** na rôzne **používateľské účty pomocou toho istého hesla**. Naopak, **brute-force útoky** sú agresívnejšie a spočívajú v **postupnom skúšaní všetkých možných kombinácií hesiel** pre konkrétne **používateľské konto**. V kontexte vyššie spomenutých útokov zohrávajú uniknuté informácie ako prihlasovacie údaje a odcudzený kryptografický materiál (napr. SSH kľúče, SSL certifikáty a pod.) kľúčový význam.

V prípade, že sa **útočníkovi** navyše **podarí získať prístup k histórii komunikácie**, tá môže byť použitá aj na prípravu cielených **spear-phishingových útokov**. **Nedostatočná reakcia v rámci riešenia incidentov,** pri ktorých došlo k úniku citlivých údajov, akú vykonala spoločnosť MICROSOFT v prípade kompromitácie svojich systémov štátom sponzorovanou skupinou **APT29,** môže viesť k ohrozeniu ďalších používateľov, zákazníkov a partnerských organizácií. Preto je dôležité v prípade ľubovoľných únikov **venovať osobitnú pozornosť zneplatneniu uniknutých hesiel a kryptografického materiálu a notifikácii zasiahnutých subjektov**. Uvedené postupy eliminujú riziko ich zneužitia v ďalších útokoch.

Druhá časť útokov bola **založená na zneužití bezpečnostných zraniteľností**. Táto skupina útokov často vyžaduje použitie sofistikovaných postupov a nástrojov. Počas aprílových útokov sa **hackeri snažili o zneužitie kritických bezpečnostných zraniteľností** v proprietárnom operačnom systéme **PAN-OS od spoločnosti PALO ALTO** a vo firewalloch **ASA a FTD od spoločnosti CISCO**. Z hľadiska prevencie týchto útokov je kľúčové venovať pozornosť zavedeniu a **prevádzkovaniu manažmentu aktív**, **manažmentu bezpečnostných zraniteľností a politík pravidelnej a riadenej aktualizácie systémov**. Dôležité je si uvedomiť, že útočníci, najmä štátom sponzorované **APT skupiny**, **na prienik do systémov často využívajú** práve **bezpečnostné**

zraniteľnosti neaktualizovaných zariadení a systémov. Ako príklad možno uviesť skupinu **APT28, ktorá v súčasnosti zneužíva zraniteľnosť CVE-2022-38028** z roku 2022.

Kontroverziu spôsobil aj nedávny **ransomvérový útok na americkú spoločnosť UNITEDHEALTH GROUP.** Tá koncom apríla 20224 potvrdila, že v súvislosti s ransomvérovým útokom z konca februára 2024 **skupine RANSOMHUB zaplatila výkupné**. Svoje rozhodnutie odôvodnila potrebou zabezpečenia kontinuity poskytovania služieb a ochrany citlivých údajov pacientov. **Hackerská skupina po zaplatení výkupného odstránila zverejnené dokumenty zo svojej webovej stránky**. **RANSOMHUB začala byť aktívna** len pomerne nedávno a odstránením obsahu po zaplatení **sa snaží ukázať**, **že dodržiava svoje deklarované postupy a budovať tým svoju „dôveryhodnosť".** Tento prípad môže u potenciálnych obetí vytvoriť nebezpečný precedens, že v prípade zaplatenia výkupného ransomvérové skupiny zasiahnuté systémy dešifrujú a uniknuté dáta nezverejnia. **Vládna jednotka CSIRT.SK v prípade ransomvérových incidentov obetiam dôrazne odporúča neplatiť útočníkovi, nakoľko neexituje žiadna záruka, že po zaplatení útočník dodrží svoje sľuby a zasiahnuté súbory naozaj dešifruje**.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci apríl riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK.

Objavila sa nová spear-phishingová kampaň, v ktorej útočníci zneužívajú meno Advokátskej kancelárie Ficek & Partners. Pod zámienkou exekučného konania vo veci úveru sa snažia presvedčiť obeť, aby otvorila PDF prílohu a klikla v nej na odkaz, ktorý má viesť na úradné dokumenty s bližšími informáciami. Odkaz však obsahuje škodlivý kód, ktorý vo finálnej fáze stiahne do zariadenia obete trójskeho koňa pre vzdialený prístup (RAT) Remcos.

Vládna jednotka CSIRT prijala v apríli hlásenie útokov typu DDoS (zneprístupnenie služby) na dve organizácie v konštituencii CSIRT.SK. Útokom sa na svojich kanáloch pochválila skupina CyberArmyofRussia_Reborn, ktorú niektoré zdroje spájajú s operáciami APT skupiny Sandworm operujúcej pod ruskou vojenskou rozviedkou GRU.

Aj tento mesiac prijala jednotka hlásenie incidentu spojeného s nasadením malvéru pre ťažbu kryptomien na kompromitovaných serveroch s už nepodporovanou verziou systému Windows. Útočníci sa na zariadenia dostali pravdepodobne zneužitím povoleného protokolu RDP.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén.

Významné útoky vo svete

Rozsiahla password-spraying kampaň

Spoločnosť CISCO upozornila na rozsiahlu password-spraying kampaň cielenú na RAVPN (Remote Access VPN) služby na zariadeniach CISCO SECURE FIREWALL, VPN služby od výrobcov FORTINET, PALO ALTO, SONICWALL a webové aplikácie používajúce AD (Active Directory) pre autentifikáciu. Počas tohto typu útoku sa útočník pokúša o prihlásenie na rôzne používateľské účty prostredníctvom rovnakého hesla. Nezávislí bezpečnostní výskumníci dokonca zverejnili informácie, na základe ktorých uvedená aktivita môže súvisieť s činnosťou ruskej štátom sponzorovanej skupiny APT29 a botnetom BRUTUS, ktorý v súčasnosti využíva viac ako 20 000 IP adries po celom svete. V súvislosti s touto aktivitou, Vládna jednotka CSIRT zverejnila na svojej webovej stránke varovanie.

Phishingové útoky na sektor zdravotníctva v Spojených štátoch

Hackerské skupiny vykonávajú sofistikované phishingové útoky na subjekty v sektore zdravotníctva v Spojených štátoch. Na obchádzanie multifaktorovej autentifikácie (MFA) používajú viacero metód, vrátane MFA bombing-u, SIM swapping-u a dokonca aj telefonického kontaktovania IT podpory s požiadavkou na pridanie ďalších zariadení pre MFA. Pri týchto volaniach na overenie identity útočníci zneužívajú nielen verejne dostupné, ale aj ukradnuté citlivé údaje. Na zvýšenie dôveryhodnosti využívajú dokonca hlas generovaný pomocou nástrojov umelej inteligencie. Pomocou viacerých opatrení, ako sú školenie zamestnancov, viacfaktorová autentifikácia a monitorovanie dátových únikov, je možné zmierniť riziko súvisiace s týmto typom útokov. Využitie AI na generovanie deepfake video a hlasových záznamov predstavuje významné riziko aj pre kybernetický priestor SR.

Nový spôsob zneužitia platformy GITHUB pre šírenie malvéru

Útočníci zneužívajú funkcionalitu vyhľadávania v repozitároch platformy GITHUB a v rámci rozsiahlej kampane zneužívajú špeciálne vytvorené súbory Visual Studio Project (prípony .csproj a .vcxproj) na šírenie malvéru KEYZETSU. Cielenou voľbou mena repozitára a špeciálnymi postupmi, akými sú napr. pravidelná aktualizácia a pridávanie kódu, like-ovanie a pod., útočníci dokážu svoje repozitáre dostať na popredné miesta vo vyhľadávaní a následne zneužiť nepozornosť obetí. Analýza spoločnosti CHECKMARX informuje, že finálny malvér je doručovaný na základe geolokácie IP adries obetí. Vývojárom a organizáciám bezpečnostní výskumníci odporúčajú, aby boli obozretní pri používaní open-source-ových knižníc a balíkov a aby pravidelne kontrolovali ich zdrojový kód na prítomnosť nezrovnalostí alebo podozrivého kódu.

CISA nariadila mitigáciu následkov januárového útoku ruskej APT29 na MICROSOFT

Agentúra pre kybernetickú bezpečnosť a bezpečnosť kritickej infraštruktúru CISA nariadila vládnym subjektom v Spojených štátoch prijať opatrenia na mitigáciu hrozieb vyplývajúcich z januárového útoku ruskej štátom sponzorovanej skupiny APT29 (MIDNIGHT BLIZZARD) na spoločnosť MICROSOFT. Hackerom sa pomocou tzv. password-spraying útoku podarilo kompromitovať e-mailové kontá zamestnancov MICROSOFT a exfiltrovať e-mailovú komunikáciu a ďalšie citlivé údaje. Historickú komunikáciu možno zneužiť na tvorbu cielených spear-phishingových kampaní a uniknuté údaje na prienik do systémov. Spoločnosť MICROSOFT v rámci riešenia incidentu nevykonala zneplatnenie uniknutých prihlasovacích údajov, čo APT29 v marci 2024 zneužila na získanie prístupu k interným systémom a repozitárom zdrojového kódu. CISA v spolupráci s MICROSOFT adresne varovala všetky subjekty ohrozené týmito únikmi a vyzvala ich k okamžitej zmene prihlasovacích údajov, zneplatneniu kryptografického

materiálu, aktivácii multifaktorovej ochrany a vykonaniu detailnej analýzy logov.

Kritická zraniteľnosť v Palo Alto PAN-OS zneužívaná už od druhej polovice marca

Kritickú zraniteľnosť v PALO ALTO PAN-OS s označením CVE-2024-3400 hackeri zneužívajú minimálne od 26. marca 2024. V súčasnosti je verejne dostupný návod na zneužitie zraniteľnosti a počet pokusov o zneužitie zraniteľnosti po jeho zverejnení podstatne vzrástol. Spoločnosť PALO ALTO opakovane upravila odporúčania na mitigáciu zraniteľnosti a vydala bezpečnostné aktualizácie pre opravu zraniteľných systémov. Útočníci po kompromitácii firewallov pokračujú hlbšie do internej siete obetí, kde sa snažia získať databázu ACTIVE DIRECTORY (ntds.dit), kryptografický materiál (DPAPI), logy udalostí (.evtx) a citlivé údaje uložené vo webových prehliadačoch. Americká agentúra CISA zraniteľnosť pridala do zoznamu aktívne zneužívaných zraniteľností. Vládna jednotka CSIRT zverejnila na svojej webovej stránke varovanie a preverila výskyt zraniteľnosti v rámci svojej konštituencie.

Iránska APT skupina MUDDYWATER inovuje riadiacu infraštruktúru

Iránska štátom sponzorovaná hackerská skupina MUDDYWATER začala používať novú C2 riadiacu infraštruktúru označenú ako DARKBEATC2. Na šírenie malvéru používa spear-phishingové správy rozposielané z kompromitovaných účtov. Správy obsahujú priamo v tele URL odkaz alebo prílohy vo formáte HTML a PDF, ktoré obsahujú odkazy na stiahnutie archívov ZIP z online úložiskových platforiem ako EGNYTE, ONEDRIVE, DROPBOX, ONEHUB a SYNC. Podľa analýzy spoločnosti DEEP INSTINCT skupina začala používať platformu EGNYTE len nedávno. Primárne riziko a úspešnosť útokov skupiny MUDDYWATER vychádza zo zneužívania citlivých údajov a histórie komunikácie získaných v rámci predchádzajúcich útokov, ktoré zvyšujú celkovú dôveryhodnosť phishingových správ používaných ako primárny vektor prieniku do systémov.

TLP: White

Pokuty pre AVAST za neoprávnené spracovanie citlivých údajov

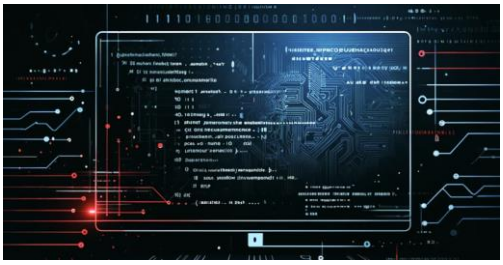
Úrad pre ochranu osobných údajov ČR uložil spoločnosti AVAST pokutu vo výške približne 14 miliónov EUR za neoprávnené spracovanie osobných údajov používateľov antivírusového softvéru AVAST a jeho rozšírení pre webové prehliadače. V roku 2019 spoločnosť poskytla časť údajov (primárne históriu webového prehliadania) vyše 100 miliónov používateľov spoločnosti JUMPSHOT, ktorá marketérom predáva informácie o správaní spotrebiteľov v online priestore. Nakoľko sa jednalo o prípad cezhraničného spracovania osobných údajov klientov zo štátov EÚ, do riešenia boli zapojené aj dozorné úrady ostatných krajín. Rovnaký prípad sa týkal aj používateľov v Spojených štátoch, kde koncom februára 2024 federálna obchodná komisia FTF spoločnosti AVAST udelila pokutu vo výške 16.5 milióna dolárov. Vzhľadom na celosvetovú popularitu softvéru boli s vysokou pravdepodobnosťou zasiahnutí aj používatelia pochádzajúci zo SR.

Mandiant pridal skupinu SANDWORM do svojho zoznamu APT skupín

Spoločnosť MANDIANT zverejnila svoju analýzu ruskej hackerskej skupiny SANDWORM, ktorú sa vzhľadom na vysokú sofistikovanosť jej činnosti rozhodla označiť za štátom sponzorovanú skupinu APT44. Skupina je aktívna približne 15 rokov a do bezpečnostného povedomia sa dostala v súvislosti s aktivitami počas konfliktu medzi Ukrajinou a Ruskom. V súčasnosti cieli na obete patriace do sektorov energetiky, telekomunikácií a verejnej správy a zameriava sa na prienik do systémov, získavanie citlivých údajov a najmä deštruktívne útoky. Analýza navyše poukázala, že APT44 svoje aktivity maskovala prostredníctvom prorusky orientovaných hacktivistických skupín XAKNET TEAM, CYBERARMYOFRUSSIA_REBORN a SOLNTSEPEK. Previazanie aktivít APT skupiny na tieto hacktivistické skupiny predstavuje riziko aj pre SR, nakoľko tieto skupiny v minulosti

vykonávali kybernetické útoky aj na subjekty v rámci SR a to minimálne v rozsahu DDoS útokov.

Severokórejská APT skupina KIMSUKI využíva AI na zvyšovanie efektivity útokov

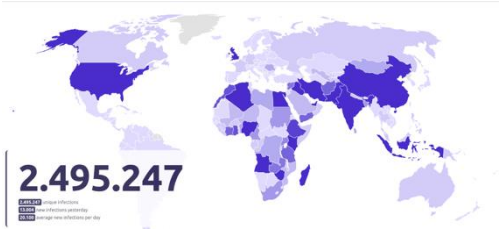


Portál THE HACKER NEWS informoval, že severokórejská štátom sponzorovaná skupina KIMSUKI nedávno začala aktívnejšie využívať dostupné technológie umelej inteligencie s cieľom zvýšenia efektívnosti a úspešnosti svojich útokov. AI nástroje využíva na sledovanie a výskum bezpečnostných zraniteľností, profilovanie obetí a generovanie obsahu šíreného v rámci dezinformačných kampaní. Po technickej stránke lokálne jazykové modely využíva na tvorbu skriptov, odstraňovanie chýb v zdrojom kóde a generovanie spear-phishingových správ. Skupina v decembri 2023 začala zneužívať nesprávne zadefinované pravidlá DMARC na spoofovanie identity a profilovanie obetí. Potvrdzuje to schopnosť APT skupiny dynamicky reagovať na aktuálne technologické trendy a prispôsobovať svoje taktiky, techniky a procedúry.

Americká UNITEDHEALTH GROUP zaplatila ransomvérovej skupine RANSOMHUB

Americká spoločnosť UNITEDHEALTH GROUP potvrdila, že v súvislosti s ransomvérovým útokom z konca februára 2024 skupine RANSOMHUB zaplatila výkupné. Svoje rozhodnutie odôvodnila potrebou zabezpečenia kontinuity poskytovania služieb a ochrany citlivých údajov pacientov. Kriminálna skupina po zaplatení výkupného odstránila zverejnené dokumenty zo svoje webovej stránky. RANSOMHUB začala byť aktívna len pomerne nedávno a odstránením obsahu sa snaží ukázať, že dodržiava svoje deklarované postupy a buduje tým svoju „dôveryhodnosť“. Celý incident vytvára nebezpečný precedens, že v prípade zaplatenia výkupného ransomvérové skupiny zasiahnuté systémy dešifrujú a uniknuté dáta nezverejnia. Vládna jednotka CSIRT v prípade ransomvérových incidentov obetiam dôrazne odporúča neplatiť útočníkovi.

Bezpečnostní výskumníci získali kontrolu nad riadiacim serverom malvéru PLUGX



Bezpečnostným výskumníkom zo spoločnosti SEKOIA sa podarilo získať kontrolu nad jedným z riadiacich serverov malvéru PLUGX a od septembra 2023 zachytiť komunikáciu z približne 2,5 miliónov unikátnych IP adries po celom svete. Výskumníci sú ochotní na požiadanie údaje poskytnúť orgánom činným v trestnom konaní a jednotkám CSIRT. Predmetnú rodinu malvéru v minulosti aktívne používala čínska štátom sponzorovaná skupina MUSTANG PANDA. Zistenia z analýzy servera poukazujú aj na výzvy jednoznačnej identifikácie kompromitovaných zariadení v prostrediach s dynamicky predeľovanými IP adresami a pri používaní VPN služieb a na ďalšie problémy, s ktorými sa v rámci riešenia incidentov stretáva aj Vládna jednotka CSIRT.

Hackeri aktívne zneužívajú zraniteľnosti v produktoch CISCO ASA a FTD

Spoločnosť CISCO varovala, že hackerská skupina UAT4356 (taktiež známa ako STORM-1849) v rámci kampane s označením ArcaneDoor aktívne zneužíva zero-day zraniteľnosti vo firewalloch/IPS Cisco ASA a FTD na prienik do vládnych systémov. Úroveň sofistikovanosti použitého malvéru (LINE DANCER, LINE RUNNER) a metód exfiltrácie citlivých údajov poukazuje, že sa pravdepodobne jedná o aktivity štátom sponzorovanej skupiny. Na uvedené zraniteľnosti sú dostupné bezpečnostné aktualizácie a návod pre overenie integrity zariadení. Vládna jednotka CSIRT na svojej webovej stránke zverejnila varovanie.

Hackeri zneužívajú chyby v platformách Github a Gitlab na šírenie malvéru

Celosvetovo populárne platformy pre vývoj softvéru a správu verzií GITHUB.COM a GITLAB.COM obsahujú chybu, ktorú útočníci aktívne zneužívajú na „pripnutie“ škodlivých súborov k existujúcim repozitárom. Pridanie súboru do komentára spôsobí jeho nahratie na servery uvedených platforiem a jeho priradenie k repozitáru, v rámci ktorého bol komentár vytvorený. Tento postup hackerom umožňuje škodlivé súbory priradiť k dôveryhodným repozitárom veľkých spoločností alebo populárnych open-source nástrojov a zvýšiť tak úspešnosť kampaní na šírenie škodlivého kódu.

Ruská APT28 aktívne zneužíva zraniteľnosť v službe Windows Print Spooler

Spoločnosť MICROSOFT zverejnila informácie, podľa ktorých ruská štátom sponzorovaná skupina APT28 dlhodobo aktívne zneužíva zraniteľnosť v službe Windows Print Spooler s označením CVE-2022-38028. Zraniteľnosť umožňuje eskaláciu privilégií a je zneužívaná v rámci útočného nástroja s označením GOOSEEGG. Analýza obsahuje detailný návod pre preverenie súvisiacich aktivít APT28 v rámci infraštruktúry s operačnými systémami Windows. Zneužitie zraniteľností v softvéri v súčasnosti predstavuje jeden z primárnych spôsobov prieniku do systémov a zdôrazňuje potrebu existencie manažmentu aktív, procesu riadenia bezpečnostných zraniteľností a politík pre pravidelnú aktualizáciu systémov.

- Kompromitovaná webová stránka Českých novín šírila dezinformácie o zmarení atentátu na prezidenta SR
- Federálny úrad pre vyšetrovanie FBI varoval amerických občanov pred využívaním nelicencovaných služieb pre prevod kryptomien
- Severokórejská APT skupina LAZARUS na šírenie malvéru používa phishingové kampane s tematikou pracovných ponúk
- Dodávateľ SMS a VoIP infraštruktúry pre službu CISCO DUO sa stal obeťou hackerského útoku, počas ktorého došlo k úniku citlivých údajov
- Americká CISA zverejnila detailnú analýzu ransomvéru AKIRA, ktorý sa šíri prevažne prostredníctvom zneužitia bezpečnostných zraniteľností
- Hackeri využívajú umelú inteligenciu ako nástroj pre tvorbu a šírenie malvéru
- Útočníci zneužívajú kompromitované stránky Wordpress na injekciu škodlivých skriptov JavaScript, ktoré slúžia na krádeže kryptopeňaženiek
- Vývojári editora Notepad++ požiadali o pomoc s odstránením phishingových domén zneužívajúcich identitu ich produktu
- Bankový trojan MISPADU rozširuje cielenie phishingových kampaní na členské štáty EÚ
- Používatelia e-mailovej služby OUTLOOK.COM zaznamenali problémy s doručovaním správ na adresátov využívajúcich službu GMAIL

Závažné zraniteľnosti bežných softvérových produktov

Ďalšie kritické zraniteľnosti v doplnkoch WordPress

Doplnky WP Automatic a WP Poll Maker obľúbenej platformy na tvorbu webových stránok obsahujú kritické zraniteľnosti, ktoré umožňujú obchádzanie autentifikácie, vzdialené vykonávanie kódu, extrakcii citlivých údajov a získanie administrátorských oprávnení. Bolo zaznamenaných viac ako 5,5 milióna pokusov o aktívne zneužitie zraniteľností.

Aktívne zneužívané zero-day zraniteľnosti Cisco

Spoločnosť Cisco poukázala na rozsiahlu kampaň pomenovanú ArcaneDoor, v ktorej útočníci zneužívajú dvoch zero-day zraniteľností CVE-2024-20353 a CVE-2024-20359. Úspešné zneužitie umožňuje útočníkom šíriť malvér a zbierať citlivé informácie v cieľovom prostredí. Cisco varovala, že sa jedná o aktívne zneužívané zraniteľnosti na firewalloch Cisco ASA a FTD hackerskou skupinou UAT4356 (alias Storm-1849). Spoločnosť zároveň opravila zraniteľnosť CVE-2024-20358, umožňujúcu injektovanie príkazov v spomínaných zariadeniach.

Kritická zraniteľnosť v doplnku WordPress

Zásuvný modul Forminator obľúbenej platformy na tvorbu webových stránok obsahuje jednu kritickú a dve vysoko závažné zraniteľnosti. Chyby umožňujú nahrať a spustiť škodlivý kód na serveri stránky, únik citlivých informácií a odmietnutie služby. Zásuvný modul využíva viac ako 500 000 stránok.

Aktívne zneužívaná zero-day zraniteľnosť v CrushFTP

Na aktívne zneužívanú bezpečnostnú chybu v produkte CrushFTP poukázal výskumník z Airbus CERT. Zero-day zraniteľnosť umožňuje neautentifikovanému útočníkovi uniknúť z virtuálneho súborového systému (VFS) a sťahovať systémové súbory. Tieto útoky sa údajne najviac zameriavali na subjekty v USA, pričom existuje podozrenie, že mohli byť politicky motivované.

TLP: White

Microsoft v rámci Patch Tuesday opravil aktívne zneužívané zraniteľnosti

Spoločnosť Microsoft opravila v rámci svojho pravidelného balíka aktualizácií Patch Tuesday 149 zraniteľností, z toho sú 3 kritické a 2 zero-day. Najzávažnejšie zraniteľnosti umožňujú eskaláciu oprávnení, vykonávanie kódu, únik informácií, či obchádzanie bezpečnostných prvkov. Zero-day zraniteľnosti CVE-2024-29988 a CVE-2024-26234 sú aktívne zneužívané.

Kritická zraniteľnosť v softvéri Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosti v softvéri PAN-OS. Verzie 10.2, 11.0 a 11.1 vo funkcii GlobalProtect obsahujú zraniteľnosť, ktorá umožňuje vzdialené vykonanie kódu. Zraniteľnosť je možné zneužiť len na firewalloch, na ktorých je zapnutá aspoň jedna z funkcií GlobalProtect Gateway alebo GlobalProtect Portal.

Zero day zraniteľnosť Google Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie na opravu jednej zero-day a troch vysoko závažných zraniteľností vo webovom prehliadači Chrome. Zraniteľnosti boli objavené počas hackerskej súťaže Pwn20wn Vancouver 2024.

Kritická zraniteľnosť v platforme Flowmon

Spoločnosť Progress vydala bezpečnostné aktualizácie platformy Flowmon pre meranie výkonnosti siete a bezpečnosti. Verzie staršie ako 11.1.14 a 12.3.5 obsahujú kritickú bezpečnostnú zraniteľnosť, ktorá umožňuje vzdialené vykonanie systémových príkazov.

Bezpečnostné zraniteľnosti v produktoch Ivanti

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 4 bezpečnostné zraniteľnosti v produktoch Connect Secure a Policy Secure. Najzávažnejšie zraniteľnosti s označením CVE-2024-21894 a CVE-2024-22053 možno zneužiť na zneprístupnenie služby a vzdialené vykonanie škodlivého kódu.

Kritická zraniteľnosť v doplnku WordPress

Doplnok obľúbenej platformy na tvorbu webových stránok obsahuje kritickú zraniteľnosť typu SQL injection, ktorá umožňuje neautentifikovaným útočníkom pripojiť ďalšie dotazy do existujúcich dotazov SQL. To môže viesť k neoprávnenému prístupu k citlivým informáciám z databázy, ako napríklad hash hesiel. Chyba sa nachádza v zásuvnom module WordPress s názvom LayerSlider.

Mesačník zraniteľností Apríl 2024

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
    - Wordpress pluginy WP Automatic a WP Poll Maker
    - Cisco Adaptive Security Appliance a Cisco Firepower Threat Defense
    - Wordpress plugin Forminator
    - CrushFTP
    - Microsoft Windows, Office, Azure, .NET Framework, Visual Studio, SQL Server, DNS Server, Windows Defender, Bitlocker a Windows Secure Boot
    - Palo Alto PAN-OS
    - Google Chrome
    - Progress Flowmon
    - Ivanti Connect Secure a Policy Secure
    - Wordpress plugin LayerSlider

https://www.csirt.gov.sk/mesacny-prehlad-kritickych-a-zavaznych-softverovych-zranitelnosti.html