CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

SEPTEMBER 2024

TLP: CLEAR





Kybernetickým priestorom v septembri 2024 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Zraniteľnosti webového portálu umožňovali získanie kontroly nad vozidlami KIA

Výskumníci v júni 2024 odhalili zraniteľnosti vo webovom portáli spoločnosti KIA, ktoré bolo možné zneužiť na získanie kontroly nad vozidlami a neoprávnený prístup k citlivým údajom.

2 TELEGRAM na základe súdnych žiadostí zdieľa údaje o používateľoch

Komunikačná platforma Telegram bude na základe upravených podmienok používania a ochrany súkromia s OČTK zdieľať informácie o používateľoch.

3 Hackeri exfiltrovali 440 GB dát zo SharePoint servera spoločnosti FORTINET

Útočník vystupujúci pod aliasom FORTIBITCH na hackerskom fóre zverejnil 440 GB dát exfiltrovaných z Azure SharePoint servera spoločnosti FORTINET.

4 Masívny botnet 7777 začína aktívne maskovať svoju prítomnosť

Prevádzkovatelia botnetu 7777 prestávajú na prístup ku kompromitovaným zariadeniam využívať doteraz známe prihlasovacie rozhrania a špecifické porty.

5 Zraniteľnosť v aplikácii WHATSAPP umožňovala obídenie mechanizmu „View Once“

Spoločnosť META vydala aktualizáciu, ktorá opravila chybu v aplikácii WHATSAPP umožňujúcu obídenie mechanizmu „View Once“ slúžiaceho na jednorazové zobrazenie správ.

6 Bezpečnostní výskumníci analyzujú podozrivú komunikáciu s napojením na Čínu

Spoločnosť GREYNOISE už od januára 2020 prostredníctvom svojej senzorovej siete zachytáva podozrivú sieťovú komunikáciu asociovanú s Čínou a prosí bezpečnostnú komunitu o pomoc s jej analýzou.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci september riešil typicky 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. Jednotka zachytila aj útoky hrubou silou na e-mailové kontá.

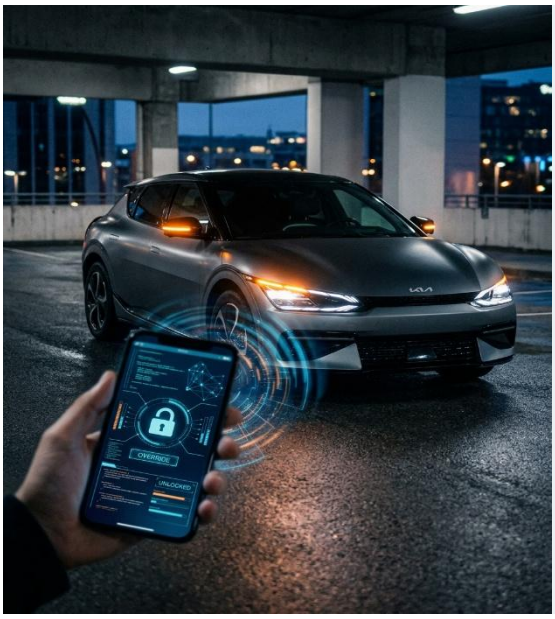
V tomto mesiaci prijala jednotka hlásenia webových skenov na webstránky niektorých organizácií a verejne dostupný logovací súbor na jednej z nich. Prístup k nemu po informovaní správcovia zamedzili. Nahlásené boli tiež zverejnené rodné čísla osôb v skenoch dokumentov, čo predstavuje únik osobných údajov a vedie k podnetu pre Úrad pre ochranu osobných údajov SR.

Zaujímavosťou boli tiež zachytené požiadavky na podozrivú doménu 'xmrig.moneroocean[.]stream' z lokality organizácie v konštituencii CSIRT.SK. Predmetné dopyty boli preverené vzhľadom na možnú kompromitáciu infraštruktúry. Ďalšie hlásenie sa týkalo podozrivých dopytov na domény smolcatkgi[.]shop a flyspecialline[.]com, ktoré sú voľne dostupnými nástrojmi označované ako škodlivé. Domény sú spájané s malvérom ClickFix.

September priniesol aj novú vlnu vyhrážok bombovými útokmi na školách. CSIRT.SK poskytol súčinnosť polícii SR pri vyšetrovaní a snahe o stotožnenie páchateľa. E-mailový účet, ktorý páchateľ použil, mal prepojenie na Telegramový účet. Incident súvisel so šírenou poplašnou správou na školách v Českej republike. Spoločným menovateľom boli adresáti, teda školské zariadenia a deklarovaný spôsob vykonania útoku. Incident prebiehal v rámci niekoľkých dní v oboch štátoch. Spoločným komunikačným kanálom zriadeným Vládnou jednotkou CSIRT došlo dňa následne k výmene informácií medzi OČTK SR a ČR, kde boli dohodnuté ďalšie postupy pri zbieraní a zdieľaní informácií, ktoré mali za úlohu pomôcť stotožniť útočníka, alebo skupinu, prípadne obmedziť ich činnosť. Indikátory kompromitácie spojené s danou e-mailovou kampaňou zdieľala jednotka CSIRT.SK so svojou konštituenciou. Zároveň všetky získané informácie a výstupy z analýzy odstúpila OČTK.

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 UDALOSTI VO SVETE



Zraniteľnosti webového portálu umožňovali odomknutie vozidiel KIA

Bezpečnostní výskumníci v júni 2024 odhalili zraniteľnosti vo webovom portáli spoločnosti KIA, ktoré bolo možné zneužiť na získanie kontroly nad vozidlami KIA a získanie neoprávneného prístupu k citlivým údajom ich majiteľov. Výskumníci vytvorili aj nástroj, ktorým po zadaní ŠPZ do 30 sekúnd dokázali vzdialene odomknúť vozidlo a interagovať s jeho internými systémami. Spoločnosť KIA zraniteľnosti odstránila a preverovanie nepotvrdilo jej zneužitie.

Google Chrome prestane od novembra 2024 dôverovať certifikátom ENTRUST

V súčasnosti je šifrovanie HTTP komunikácie s webovým serverom základom ochrany súkromia a bezpečnosti používateľov. Táto ochrana je zabezpečená certifikátmi, ktoré vydáva tzv. certifikačná autorita. Od novembra 2024 webový prehliadač GOOGLE CHROME prestane dôverovať certifikátom vydaným certifikačnou autoritou ENTRUST. Vládna jednotka CSIRT na súvisiace riziká a možné dopady na používateľov upozornila na svojej webovej stránke.

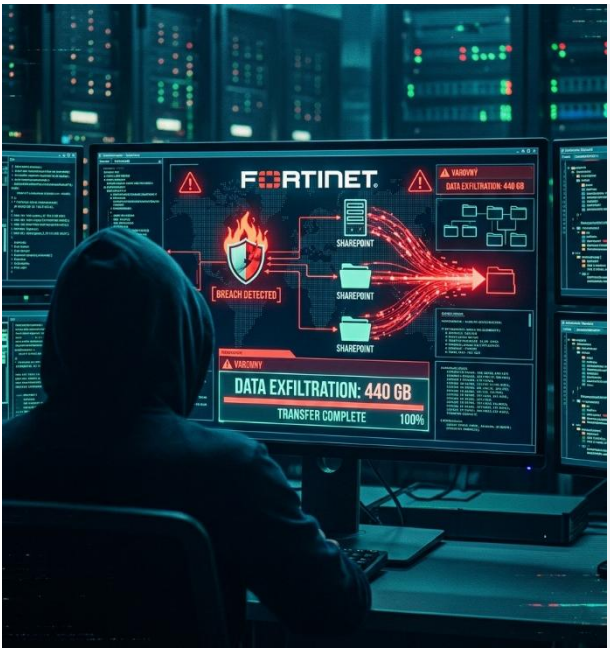




Telegram na základe súdnych žiadostí zdieľa údaje o používateľoch

CEO Pavel Durov informoval o upravených podmienkach ochrany súkromia platformy TELEGRAM, podľa ktorých bude platforma v prípade súdnych žiadostí s OČTK zdieľať IP adresu a telefónne číslo používateľov obvinených z kriminálnej činnosti. Platforma sprístupnila špeciálneho bota pre transparentné zverejňovanie informácií o počte žiadostí o zdieľaní dát a taktiež bota pre nahlasovanie ilegálneho obsahu, ktorý preverí dedikovaný tím moderátorov.

VÝZNAMNÉ UDALOSTI VO SVETE



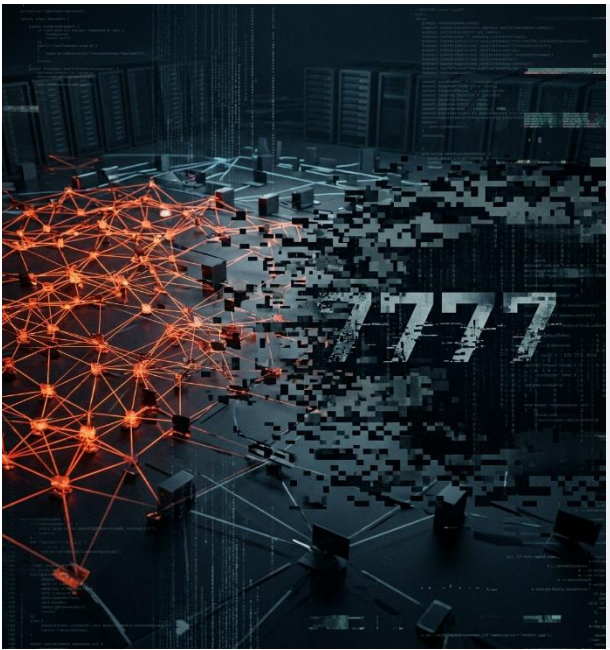
Hackeri exfiltrovali 440 GB dát zo SharePoint servera spoločnosti FORTINET

Útočník vystupujúci pod aliasom **FORTIBITCH** na hackerskom fóre zverejnil linku na Amazon S3 bucket obsahujúci 440 GB dát exfiltrovaných z Azure SharePoint servera spoločnosti FORTINET. Spoločnosť obratom potvrdila, že sa stala obeťou útoku. Zároveň upresnila, že uniknuté dáta obsahovali aj bližšie nešpecifikované dáta zákazníkov, ktorých obratom notifikovala. Nakoľko sú produkty spoločnosti Fortinet populárne aj v rámci SR, incident mohol zasiahnuť aj dáta slovenských používateľov.

Čínska skupina DRAGONRANK kompromituje Microsoft IIS servery



Bezpečnostní výskumníci z CISCO TALOS zverejnili informácie o novej kampani čínskej skupiny DRAGONRANK, ktorá je cielená štáty v Európe a Ázii. Skupina na prvotný prienik do systému zneužíva známe zraniteľnosti. Následne dochádza k umiestneniu ASPXSPY webshell-u slúžiaceho na vzdialený prístupu k zariadeniam, získavanie a exfiltráciu citlivých údajov a inštaláciu malvérov PLUGX a BADIIS. Malware BADIIS je vytvorený špecificky pre IIS servery, ktoré zapája do infraštruktúry útočníka používaného na SEO manipuláciu.



Masívny botnet 7777 začína aktívne maskovať svoju prítomnosť

Bezpečnostní výskumníci informovali o narastajúcej aktivite botnetu 7777, ktorý postupne rozširuje svoje cielenie aj na VPN zariadenia, routre a mediálne servery od výrobcov ZYXEL, RUCKUS, ASUS a AXENTRA. Botnet zároveň začal využívať dodatočné mechanizmy maskovania svojej činnosti. Útočníci začali nasadzovať pre vzdialenú kontrolu zariadení nasadzovať HTTP reverzný shell UPDATE, vďaka čomu už nemusia na prístup využívať prihlasovacie rozhrania a špecifické porty, ktoré bezpečnostná komunita využívala na identifikáciu kompromitovaných zariadení.

VÝZNAMNÉ UDALOSTI VO SVETE



Zraniteľnosť v aplikácii WhatsApp umožňovala obídenie mechanizmu „View Once“

Spoločnosť META vydala aktualizáciu, ktorá opravila chybu v aplikácii WHATSAPP umožňujúcu obídenie mechanizmu „View Once“. Podľa bezpečnostných výskumníkov bola chyba aktívne zneužívaná útočníkmi minimálne už jeden rok a počas tohto obdobia dokonca vzniklo viacero zásuvných modulov a nástrojov na deaktiváciu View Once príznaku prichádzajúcich správ, čo umožňovalo obídenie tohto bezpečnostného mechanizmu.

Severokórejská skupina LAZARUS cieli na softvérových vývojárov

Severokórejská APT skupina LAZARUS pokračuje v malwaretisement kampani VMCONNECT cielenej na softvérových vývojárov. Obete sú rôznymi spôsobmi (primárne prostredníctvom LINKEDIN) kontaktované ohľadom pracovnej ponuky a v rámci praktickej časti pohovoru im je podvrhnutý škodlivý kód distribuovaný prostredníctvom NPM, PYPI alebo GITHUB repozitárov. Nakoľko skupina tento modus operandi úspešne využíva už približne rok, jedná sa o tému, ktorej sa treba venovať v rámci zvyšovania kybernetického povedomia aj v rámci SR.





Android malvér získava prihlasovacie údaje z obrázkov na zariadení

Bezpečnostní výskumníci zverejnili analýzu Android malvéru SPYAGENT, ktorý využíva OCR (Optical Character Recognition) technológiu na extrakciu prístupových fráz ku kryptopeňaženkám a ďalších citlivých údajov priamo zo screenshotov uložených na zariadení. Malvér sa šíri prostredníctvom phishingových a smishingových kampaní zneužívajúcich identitu vládnych služieb, internetových zoznamiek a pornografických stránok. Od augusta 2024 útočníci začali vyvíjať aj variant pre iOS.

VÝZNAMNÉ UDALOSTI VO SVETE

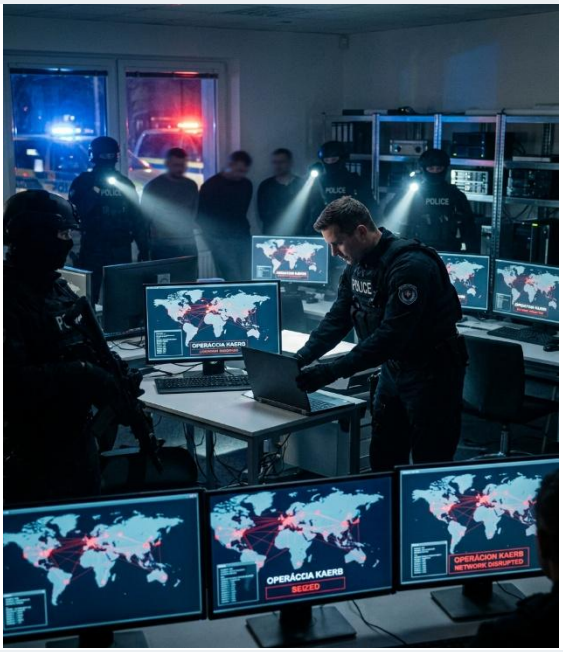


Výskumníci analyzujú podozrivú komunikáciu s napojením na Čínu

Spoločnosť GREYNOISE už od januára 2020 prostredníctvom svojej senzorovej siete zachytáva podozrivú sieťovú komunikáciu a prosí bezpečnostnú komunitu o pomoc s jej analýzou. Podľa hypotéz sa môže jednať o pozostatky utajovanej komunikácie, koordinačné signály pre DDoS, C2 komunikáciu malvéru alebo miskonfiguráciu systémov. Sieťový tok je cielený na konkrétnych poskytovateľov internetového pripojenia. Taktiež bolo zachytené veľké množstvo ICMP paketov obsahujúcich ASCII reťazec "LOVE".

Medzinárodná operácia KAERB viedla k rozloženiu kriminálnej siete

OČTK v rámci medzinárodnej akcie OPERATION KAERB rozložili medzinárodnú kriminálnu sieť, ktorá bola aktívna najmenej 5 rokov a na odblokovanie ukradnutých alebo stratených mobilných zariadení využívala phishing-as-a-service platformu ISERVER. Služba na získavanie prihlasovacích údajov vlastníkov odcudzených zariadení využívala rôzne formy phishingu, smishingu a vishingu. Táto operácia zdôrazňuje dôležitosť medzinárodnej spolupráce v boji proti kyberzločinu a potrebu neustáleho zvyšovania povedomia o kybernetickej bezpečnosti.





Aplikácia TEMU popiera únik dát

Útočník na hackerskom fóre zverejnil na predaj databázu s 87 miliónmi záznamov zákazníkov TEMU, vrátane vzorovej sady dát. Spoločnosť TEMU na základe analýzy obsahu vzorky poprela, že by došlo ku kompromitácii ich systémov a exfiltrácii dát a celú situáciu označilo ako pokus o poškodenie svojej reputácie. Nakoľko dáta obsahujú citlivé údaje ako používateľské mená, IP adresy, adresy a hashe hesiel, používatelia TEMU by mali v rámci prevencie aktivovať MFA a vykonať preventívnu zmenu prihlasovacích údajov.

VÝZNAMNÉ UDALOSTI VO SVETE



Spojené štáty zaistili 32 domén šíriacich proruskú propagandu

Ministerstvo spravodlivosti USA informovalo o zaistení 32 domén, ktoré boli v rámci operácie DOPPELGÄNGER zneužívané na šírenie proruskej propagandy. Cieľom hybridného pôsobenia aktérov je znížiť medzinárodnú podporu Ukrajiny, pretláčať proruské záujmy a ovplyvniť výsledky nadchádzajúcich prezidentských volieb. Útočníci zneužívajú influencerov, platené reklamy na sociálnych médiách a falošné profily, ktoré zdieľajú odkazy na domény s manipulatívnym obsahom. Mnohé zaistené domény imitovali legitímne publicistické a spravodajské portály.

Európske banky pod útokom nového variantu malvéru

Bezpečnostní výskumníci zverejnili analýzu novej verzie Android malwaru OCTO2, ktorý sa v Európe šíri vo forme aplikácií zneužívajúcich identitu NordVPN, Google Chrome a Europe Enterprise. Malvér k legitímnym APK súborom prostredníctvom služby ZOMBIDER pridáva škodlivý payload, čím je zachovaná pôvodná funkcionalita softvéru. Kampaň bola zachytená v Taliansku, Poľsku a Maďarsku. Vládna jednotka CSIRT odporúča inštalovať mobilné aplikácie výhradne prostredníctvom oficiálnej aplikácie GOOGLE PLAY.





WORDPRESS.ORG blokuje prístup WP Engine k svojím zdrojom

WORDPRESS.ORG zakázala prístup k zdrojom a prestala doručovať aktualizácie pluginov na webové stránky hostované na platforme WP Engine. Platforma mala modifikovať jadrové funkcie redakčného systému k vlastnému prospechu a blokovať dashboard so správami, aby sa používatelia nedozvedeli o stanovisku wordpress.org. Stránky prevádzkované na uvedenej platforme sú bez bezpečnostných aktualizácií, vystavené zvýšenému riziku útokov a administrátori by mali zvážiť migráciu na iný hosting.

VÝZNAMNÉ UDALOSTI VO SVETE



Marketingová kampaň v Spojenom kráľovstve poukazuje na riziká QR kódov

V Spojenom kráľovstve bola zachytená úspešná marketingová kampaň, ktorá priamo poukázala na bezpečnostné riziká spojené s narastajúcim používaním QR kódov. Pri interakcii s QR kódmi je potrebné vždy overiť zdroj QR kódu, vykonať jeho vizuálnu kontrolu, na skenovanie používať dôveryhodné aplikácie a byť opatrní v prípade žiadostí o zadanie citlivých údajov.

VÝZNAMNÉ UDALOSTI VO SVETE

- Útočníci používajú supply chain útok "Revival Hijack", pri ktorom registrujú nové PyPi projekty pod názvom balíkov, ktoré boli v minulosti odstránené
- Newyorská nezisková organizácia Planned Parenthood, ktorá sa venuje reprodukčnej medicíne a vzdelávaniu v tejto oblasti, sa stala obeťou ransomvérového útoku
- USA uvalili sankcie na prokremeľskú stanicu Russia Today (RT), pričom obvinili niekoľkých zamestnancov z údajnej snahy ovplyvniť nadchádzajúce prezidentské voľby v USA
- Ruská spoločnosť DR.WEB informovala, že sa 14. septembra 2024 stala obeťou kybernetického útoku, v rámci ktorého bližšie nešpecifikovaný útočník získal neoprávnený prístup k IT infraštruktúre spoločnosti
- Útočník na hackerskom fóre zverejnil údaje vyše 10 000 zamestnancov a partnerských subjektov spoločnosti DELL.
- Slovenská informačná služba môže disponovať nástrojom Pegasus, teda špionážnym softvérom nasadzovaným do mobilných telefónov záujmových osôb
- Ministerstvo vnútra SR zverejnilo infografiku zachytávajúcu odporúčaný postup, čo robiť pri hrozbe bombového útoku.
- Bezpečnostní výskumníci informovali o malwaretisement kampani kyberkriminálnej skupiny MARKO POLO, ktorá slúži na šírenie vyše 50 rôznych typov malvérov
- Ukrajina zakázala využívanie aplikácie TELEGRAM v rámci vládnych organizácií, vojenských jednotiek a subjektov patriacich do kritickej infraštruktúry štátu
- Bezpečnostní výskumníci zverejnili informácie o infraštruktúre iránskych hackerov, ktorá je zneužívaná v rámci útokov súvisiacich s nadchádzajúcimi prezidentskými voľbami v USA
- Útočníci zneužívajú komentáre na platforme GITHUB ohľadom riešenia problémov a chýb na šírenie malwaru LUMMA STEALER, ktorého cieľom je kradnúť citlivé informácie.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v Apache Open For Business

V aplikácii Apache Open For Business bola opravená kritická zraniteľnosť umožňujúca vzdialené vykonávanie kódu bez potreby autentifikácie. Súvisí s nedostatočným overením oprávnení používateľa, ktorý sa pokúša priamo pristúpiť ku chráneným zdrojom.

Cisco opravuje dve kritické zraniteľnosti v Smart Licensing Utility

Aplikácia Cisco Smart Licensing Utility obsahuje dve kritické zraniteľnosti, ktoré umožňujú útočníkom získať prihlasovacie údaje pre prístup k API rozhraniu s administrátorskými oprávneniami.

Kritické zraniteľnosti v produktoch Veeam

Spoločnosť Veeam opravila kritické zraniteľnosti v produktoch Backup & Replication (VBR), ONE, Service Provider Console a ďalších. Najzávažnejšia z nich umožňuje neautentifikovanému útočníkovi vzdialene vykonávať kód vo VBR. V balíku opráv spoločnosť vyriešila aj viacero ďalších vysoko závažných zraniteľností.

Bezpečnostné zraniteľnosti v produkte Ivanti Endpoint Management

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 16 bezpečnostných zraniteľností v produkte Endpoint Manager, z čoho 10 je označených ako kritických. Kritické zraniteľnosti možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Ostatné zraniteľnosti možno zneužiť na eskaláciu privilégií, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Media Encoder, Audition, After Effects, Premiere Pro, Illustrator, Acrobat Reader, ColdFusion a Photoshop, ktoré opravujú 29 zraniteľností, z čoho 19 sú označené ako kritické. Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vzdialené vykonanie škodlivého kódu. Ostatné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vykonanie neoprávnených zmien v systéme a zneprístupnenie služby.

Microsoft v rámci septembrového Patch Tuesday opravil 7 kritických zraniteľností

Spoločnosť Microsoft vydala v septembri 2024 balík opráv pre portfólio svojich produktov opravujúci 79 zraniteľností, z ktorých 19 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v produktoch Microsoft SharePoint Server, Azure Web Apps a Azure Stack Hub a v komponentoch Windows Network Address Translation a Microsoft Windows Update a možno ich zneužiť na eskaláciu privilégií a vzdialené vykonanie škodlivého kódu. Zraniteľnosti s označením CVE-2024-38014, CVE-2024-38217, CVE-2024-38226, CVE-2024-43491 v Microsoft Publisher a komponentoch Windows Installer, MOTW (Mark of the Web) a Windows Update sú aktívne zneužívané útočníkmi.

GitLab opravuje kritickú a vysoko závažné zraniteľnosti

Spoločnosť GitLab vydala opravný balík pre 18 zraniteľností. Z toho jedna je hodnotená ako kritická a tri ako vysoko závažné. Chyby umožňujú vzdialene vykonávať príkazy, spôsobiť nedostupnosť služby alebo vykonať útoky typu SSRF (Server-side request forgery).

Vysoko závažné zraniteľnosti v Cisco IOS XR

Spoločnosť CISCO vydala bezpečnostné aktualizácie na svoj operačný systém IOS XR, ktoré opravujú 8 zraniteľností, z čoho 6 je označených ako vysoko závažné. Zraniteľnosti s označením CVE-2024-20398, CVE-2024-20304, CVE-2024-20483, CVE-2024-20489, CVE-2024-20317 a CVE-2024-20406 možno zneužiť na injekciu príkazov, vykonanie škodlivého kódu, eskaláciu privilégií, zneprístupnenie služby a získanie neoprávneného prístupu k citlivým údajom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti routerov D-Link

Spoločnosť D-Link opravila tri kritické a dve vysoko závažné zraniteľnosti vo firmvéroch zariadení COVR-X1870, DIR-X4860 a DIR-X5460. Zraniteľnosti súvisia s napevno kódovanými prihlasovacími údajmi a ďalšími chybami, ktoré umožňujú vzdialene vykonávať kód, pristupovať k zariadeniam cez Telnet a vykonávať systémové príkazy.

Kritická zraniteľnosť vo VMware vCenter Server

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, opravujúce bezpečnostné chyby ovplyvňujúce VMware vCenter Server. Z nich 1 je označená ako kritická a 1 vysoko závažná. Zraniteľnosti možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu.

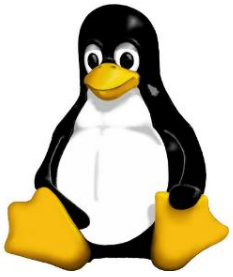
Kritická zraniteľnosť GitLab

Spoločnosť GitLab vydala aktualizáciu opravujúcu kritickú zraniteľnosť, ktorá zasahuje autentifikačný proces na báze štandardu SAML. Chyba umožňuje neoverenému útočníkovi obísť prihlásenie.

Útočníci zneužívajú kritickú zraniteľnosť Ivanti Cloud Services Appliance

Spoločnosť Ivanti informovala o novej kritickej zraniteľnosti v produkte CSA, ktorá umožňuje získať prístup ku chráneným funkcionalitám. Útočníci ju zneužívajú v kombinácii s nedávno publikovanou zraniteľnosťou umožňujúcou vzdialené vykonávanie kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV



Kritická a závažné zraniteľnosti OpenPLC

Kyberbezpečnostná jednotka Talos spoločnosti Cisco zverejnila podrobnosti o viacerých opravených zraniteľnostiach v programovateľnom logickom ovládači OpenPLC, ktoré možno zneužiť pri útokoch DoS a na vzdialené vykonávanie kódu.

Zraniteľnosti v tlačovom subsystéme pre Unix a Linux možno zneužiť na vzdialené vykonanie kódu

Implementácia internetového tlačového protokolu IPP pre unixové systémy CUPS obsahuje 4 zraniteľnosti, z ktorých jedna je označená ako kritická. Zreťazením zraniteľností by vzdialený neautentifikovaný útočník mohol získať kontrolu nad parametrami v súbore PPD a možnosť vzdialene vykonávať kód.

MESAČNÍK ZRANITEĽNOSTÍ SEPTEMBER 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
   - CUPS (Common UNIX Printing System) komponenty cups-filters, libcupsfilters, libppd, cups-browsed
   - OpenPLC
   - Ivanti CSA (Cloud Services Appliance)
   - GitLab Community Edition (CE), GitLab Enterprise Edition (EE)
   - VMware vCenter Server, VMware Cloud Foundation
   - D-Link routre COVR-X1870, DIR-X4860, DIR-X5460
   - Cisco IOS XR
   - Azure CycleCloud, Azure Network Watcher VM Extension for Windows, Azure Stack Hub, Azure Web Apps, Microsoft 365, Microsoft AutoUpdate for Mac, Microsoft Dynamics 365, Microsoft Excel, Microsoft Office, Microsoft Publisher, Microsoft SQL Server, Microsoft SharePoint, Microsoft Visio, Outlook for iOS, Power Automate for Desktop, Windows, Windows Server
   - Adobe Media Encoder , Adobe Audition, Adobe After Effects, Adobe Premiere Pro, Adobe Illustrator 2024, Acrobat DC, Acrobat Reader DC, Acrobat 2024, Acrobat 2020, Acrobat Reader 2020, ColdFusion 2023, ColdFusion 2021, Photoshop 2023, Photoshop 2024
   - Ivanti Endpoint Manager
   - Veeam Backup & Replication, Veeam Service Provider Console, Veeam ONE, Veeam Agent for Linux, Veeam Backup for Nutanix AHV Plug-In, Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization Plug-In
   - Cisco Smart License Utility
   - Apache OFBiz

https://csirt.sk/posts/1412.html