CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

OKTÓBER 2024

TLP: CLEAR

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

1 Ruská APT29 v rámci spear-phishingových útokov zneužíva škodlivé .RDP súbory

Ruská hackerská skupina APT29 na prienik do systémov vládnych a vojenských cieľov zneužíva e-mailové správy, ktoré v prílohe obsahujú škodlivé súbory na konfiguráciu vzdialeného prístupu.

2 CSIRT odhalil SQL injection zraniteľnosť vo frameworku Nette

Bezpečnostní analytici VJ CSIRT.SK objavili potenciálnu zraniteľnosť vo webovom frameworku Nette, ktorá umožňuje vykonávať útoky typu SQL injection.

3 Útočníci ukradli dáta 31 miliónov používateľov služby ARCHIVE.ORG

Neznámy útočník kompromitoval systémy internetového archívu ARCHIVE.ORG a exfiltroval prihlasovacie údaje približne 31 miliónov používateľov služby.

4 Rozmach zneužívania QR kódov v rámci phishingových útokov

Bezpečnostní výskumníci zo spoločnosti BARRACUDA upozornili na pokračovanie rastúceho trendu zneužívania QR kódov v rámci phishingových útokov a nové metódy ich maskovania.

5 Phishingové e-maily zneužívajúce identitu izraelského distribútora produktov ESET

Hackeri prenikli do systémov izraelského distribútora produktov spoločnosti ESET a zneužili ich na rozposielanie phishingových e-mailov šíriacich deštruktívny malvér.

6 Globálna malwaretisement kampaň zameraná na podnikové účty a stránky META

Útočníci na šírenie a riadiacu komunikáciu malvéru SYS01STEALER zneužívajú kompromitované FACEBOOK kontá, webové stránky a reklamnú platformu spoločnosti META.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej činnosti CSIRT.SK v mesiaci október 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.

Opäť sa objavili phishingové e-maily cieliace na zákazníkov slovenských bánk. V jednom prípade sa jednalo o "kampaň Poštovej banky" a súčasťou bol odkaz na podvrhnutý webový formulár, ktorý ukladal po vyplnení vstupov prihlasovacie údaje obete na server do súboru vo formáte „txt“. CSIRT.SK kontaktoval správcov hostingu s požiadavkou o stiahnutie škodlivého obsahu, a súčasne informoval tímy SK-CERT a SOC NASES.

Začiatkom mesiaca prijala Vládna jednotka CSIRT hlásenie o e-maile s vyhrážkou únosu civilného lietadla, s ktorým mali odosielatelia zaútočiť na elektráreň v Mochovciach. Výhražná správa niesla znaky operácie v rámci aktuálnych hybridných hrozieb. VJ CSIRT vypracovala analýzu získaných podkladov a informácie poskytla OČTK aj svojim zahraničným partnerom.

Na základe informácie o kompromitovaných zariadeniach zapojených do SSH botnetu, ktorú jednotke poskytla polícia SR, CSIRT.SK vypracoval analýzu kriminálnej skupiny GXC TEAM, ktorá poskytuje služby malware-as-a-service. Jedná sa o phishingové frameworky so škodlivými aplikáciami pre Android. Škodlivý kód po inštalácii pýta povolenie byť predvolenou aplikáciou pre SMS, čo útočníkom umožňuje zachytávanie a exfiltráciu citlivých údajov, vrátane OTP kódov, prostredníctvom TELEGRAM botov. K ďalším funkcionalitám patrí aj zobrazenie phishingu prostredníctvom WEBVIEW. Framework umožňuje aj generovanie hlasových hovorov prostredníctvom AI nástrojov.

V rámci hrozieb na úrovni štátnych aktérov bola zaznamenaná komunikácia v rámci konštituencie VJ CSIRT, ktorá súvisela s aktuálnou širšou kampaňou ruskej štátom sponzorovanej skupiny APT29, zameranou na vládne a vojenské organizácie. Skupina v rámci kampane cieli na exfiltráciu prihlasovacích údajov a dát.

CSIRT.SK riešil v októbri tiež nezvyčajnú komunikáciu zo strany organizácie vo svojej konštituencii, ktorú vyhodnotil ako automatické preposielanie e-mailových správ na nelegitímnu adresu geolokalizovanú v Číne, ktorú útočníci nastavili po kompromitácii e-mailového servera. Preposielanie živej komunikácie bolo uskutočnené vo veľkom množstve (cca 1700 správ) s kompletnými prílohami, osobnými údajmi a všetkým čo správy obsahovali. Po analýze jednotka zahájila spoluprácu s kolegami z SK-CERT.

Aj v októbri sa vyskytol prípad webstránky používajúcej neaktuálnu verziu redakčného systému WordPress. Stránka mala dostupné administrátorské rozhranie na [.../wp-login.php] z internetu. CSIRT.SK všeobecne odporúča obmedziť prístup k administračným rozhraniam webstránok

a služieb dostupných z internetu aby sa znížilo riziko útokov vedúcich k neoprávneného prístupu a získaniu kontroly nad týmito službami.

Okrajovo sa jednotka CSIRT.SK stretla s investičným podvodom, ktoré sú v našej krajine v poslednom období rozšírené. Podvod funguje nasledovne. Zavolá Vám cudzie číslo, v časti prípadov slovenské, v časti zahraničné. V dobrej slovenčine so silným rusko-ukrajinsko-bulharským prízvukom Vás volajúci informuje, že máte v ich spoločnosti neaktívny investičný účet s kryptomenami v hodnote niekoľko tisíc alebo desiatok tisíc Eur, z ktorého si musíte vybrať peniaze, inak bude zrušený. Vo veľkej časti prípadov sa domnelá spoločnosť nazýva „Investing.com“ alebo „Blockchain“. Podvodníci môžu následne požadovať prístup k Vášmu zariadeniu, do Vášho bankového účtu alebo Vás môžu presviedčať, aby ste zainvestovali ďalšie peniaze. V spomínanom prípade nastala obeti škoda približne 66 000 Eur, ktoré boli prevedené na Revolut a na kryptomeny cez účty na burze Binance.

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.

V októbri CSIRT.SK plošne varoval svoju konštituenciu ohľadom zneužívania platformy 500apps.com vo phishingových kampaniach. Adresne varoval organizácie ohľadne zneužívanej zraniteľnosti CVE-2024-23113 Fortinet FFGFMD.

CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj študentom stredných škôl. V októbri prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Bratislavského samosprávneho kraja, študentom SOŠ Podnikateľskej v Senici, SPŠ Strojníckej Fajnorka v Bratislave, Gymnázia v Pezinku a tiež študentom a učiteľom Gymnázia Šrobárova v Košiciach.

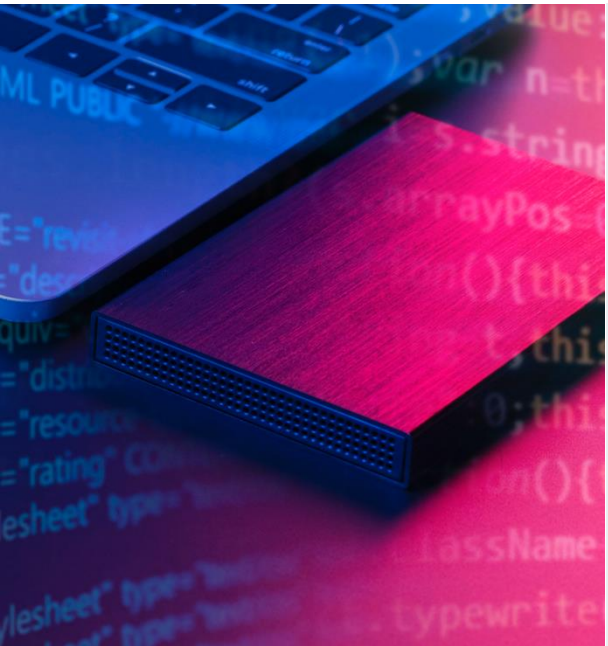
VÝZNAMNÉ UDALOSTI VO SVETE

Ruská APT29 v rámci spear-phishingových útokov zneužíva škodlivé .RDP súbory

Spoločnosť AMAZON zaistila domény asociované s aktivitami ruskej APT29 cielenými na vládne a vojenské organizácie, v rámci ktorých skupina na exfiltráciu prihlasovacích údajov a dát zneužívala .RDP súbory obsahujúce nastavenia profilu pre spojenie. Po otvorení vytvárali RDP spojenie so servermi útočníka, v rámci ktorého profil zdieľal lokálne súbory, sieťové zdroje, tlačiarne, COM porty, audio zariadenia a obsah schránky. Na základe dostupných informácií phishingová kampaň cielila na viaceré štáty, pričom najväčší dopad mala na Ukrajinu a Českú republiku.

Šírenie phishingových e-mailov cez izraelského distribútora produktov ESET

Bližšie nešpecifikovaní hackeri prenikli do systémov izraelskej spoločnosti COMSECURE, ktorá je lokálnym distribútorom spoločnosti ESET, a zneužili ich na rozposielanie phishingových e-mailov slúžiacich na šírenie deštruktívneho wiperu. Útok, ktorý začal 8. októbra, zneužil značku ESET a e-mailovú doménu distribútora jej produktov na vytvorenie dôveryhodného dojmu. E-mail obeť upozornil, že je cieľom APT skupiny, a v tele obsahoval URL odkaz na stiahnutie ZIP archívu s malvérom vydávajúcim sa za „pokročilejšiu“ verziu produktov ESET. Rozsah a úspešnosť kampane zatiaľ nie sú známe.



CSIRT.SK odhalil SQL injection zraniteľnosť vo frameworku Nette

Bezpečnostní analytici VJ CSIRT.SK objavili potenciálnu zraniteľnosť vo webovom frameworku Nette, ktorá umožňuje vykonávať útoky typu SQL injection. Zraniteľnosť sa nachádza v knižnici Database a súvisí s absenciou ošetrovania používateľských vstupov, ktoré preberá funkcia where($by). Táto metóda podporuje filtrovanie výsledkov databázovej požiadavky podľa poľa, v ktorom kľúče predstavujú názvy stĺpcov a hodnoty daných kľúčov predstavujú požadované hodnoty. Útočník môže vykonať útok typu SQL injection podvrhnutím kľúča premennej priamo v URL v prehliadači alebo v závislosti od konkrétneho prípadu aj vo vstupoch aplikácie.

VÝZNAMNÉ UDALOSTI VO SVETE

OČTK v rámci OPERATION MAGNUS rozložili infraštruktúru REDLINE a META

Holandská polícia s partnermi v rámci medzinárodnej akcie OPERATION MAGNUS rozložili sieťovú infraštruktúru infostealerov REDLINE a META, ktoré sa zameriavali na získavanie citlivých údajov. V rámci akcie boli zaistené zdrojové kódy, licenčné servery, prihlasovacie údaje, IP adresy, registračné a ďalšie bližšie nešpecifikované údaje, ktoré OČTK môžu využiť na identifikáciu a následné zatknutie útočníkov. Hlavným technickým konzultantom operácie bola spoločnosť ESET, ktorá OČTK upozornila na vyše 1200 serverov asociovaných s činnosťou malwarov a neskôr zverejnila nástroj na vyhodnotenie, či bolo zariadenie infikované uvedenými rodinami malwaru.

MS využíva Azure inštancie ako honeypoty pre mapovanie aktivít útočníkov

Spoločnosť MICROSOFT začala vytvárať honeypot AZURE inštancie slúžiace na zber informácií o moduse operandi a mapovanie infraštruktúry útočníkov. Jedná sa o vysoko interaktívne honeypoty simulujúce rozsiahlu infraštruktúru spoločnosti, vrátane domén, používateľských kont a interného zdieľania súborov. Na rozdiel od klasických prístupov založených na čakaní útoku výskumníci do phishingových formulárov aktívne zadávajú prihlasovacie údaje do honeypotov, čím akcelerujú celý proces útoku. Informácie boli odprezentované v rámci konferencie BSIDES EXETER.

Prienik do systémov spoločnosti MoneyGram, únik informácií

Služba na prevod peňazí MONEYGRAM dokončila vyšetrovanie kybernetického útoku, ktorý mal v septembri 2024 za následok 5-dňovú nedostupnosť služieb. Služba je prevádzkovaná vo vyše 200 štátoch, vrátane SR. Analýza potvrdila prienik do interných systémov a že v rámci útoku došlo aj k exfiltrácii citlivých údajov používateľov služby. Uniknúť mali dáta o transakciách, kontaktné údaje zákazníkov, preukazy totožnosti a čísla bankových účtov. Podľa dostupných informácií útočník na prienik do systémov zneužil prihlasovacie údaje pracovníka helpdesku a na základe modusu operandi sa mohlo jednať o aktivity hackerskej skupiny SCATTERED SPIDER.

VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci ukradli dáta 31 miliónov používateľov z Archive.org

Neznámy útočník kompromitoval systémy internetového archívu ARCHIVE.ORG, do stránok injektoval JavaScript kód informujúci o prieniku a exfiltroval obsah databázy pre autentifikáciu používateľov. Prevádzkovateľ služby Have I Been Pwned potvrdil, že od útočníka dostal 6,4 GB SQL súbor obsahujúci prihlasovacie údaje približne 31 miliónov používateľov služby. ARCHIVE.ORG sa tento týždeň stal aj cieľom rozsiahleho DDoS útoku, ku ktorému sa prostredníctvom sociálnej siete Twitter prihlásila hacktivistická skupina BLACKMETA. Používateľom predmetnej služby CSIRT.SK odporúča vykonať bezodkladnú zmenu hesla.

Rozmach zneužívania QR kódov v rámci phishingových útokov.

Bezpečnostní výskumníci zo spoločnosti BARRACUDA upozornili na dve nové metódy maskovania URL odkazov v rámci phishingových útokov. Prvá je založená na zneužití QR kódov, ktoré nie sú vkladané vo forme statických obrázkov, ale sú vystavené prostredníctvom sekvencie špeciálnych ASCII/UNICODE znakov v texte, čo znemožňuje bezpečnostným prvkom extrakciu URL. Druhá je založená na využití BLOB URI, ktoré umožňujú v prehliadači zobraziť obsah vytvorený na základe lokálne generovaných dát. Analyzované kampane upozorňujú na pokračovanie rastúceho trendu zneužívania QR kódov v phishingových kampaniach.

Zneužívanie pentestovacieho nástroja EDRSilencer v rámci útokov

Bezpečnostní výskumníci informovali, že útočníci začínajú vo zvýšenej miere zneužívať open-source pentestovací nástroj EDRSILENCER, ktorý slúži na identifikáciu antivírusových a bezpečnostných riešení inštalovaných na zariadeniach obetí a následnú deaktiváciu hlásení zasielaných do manažmentových konzol. Aktuálna verzia nástroja je schopná identifikovať procesy súvisiace s činnosťou 16 rôznych EDR riešení a prostredníctvom platformy WFP (Windows Filtering Platform) ich podľa potreby monitoruje a blokuje ich sieťovú prevádzku. Spoločnosť TREND MICRO navrhla, aby antivírusové riešenia tento nástroj označili za malvér.

VÝZNAMNÉ UDALOSTI VO SVETE

Kompromitované WordPress stránky zneužívané na získanie citlivých údajov

Bezpečnostní výskumníci informovali o kompromitácii vyše 6 000 webových stránok založených na redakčnom systéme WORDPRESS, ktoré útočníci ďalej zneužívajú v rámci kampaní CLEARFIX (upozornenie na problém, riešením je skopírovať a spustiť skript v príkazovom riadku) a CLEARFAKE (zobrazenie falošného upozornenia na aktualizáciu prehliadača) slúžiacich na šírenie infostealerov. Útočníci inštalujú škodlivé pluginy redakčného systému imitujúce názvy populárnych pluginov a na pozadí do zdrojového kódu injektujú skripty pre zobrazenie škodlivého obsahu.

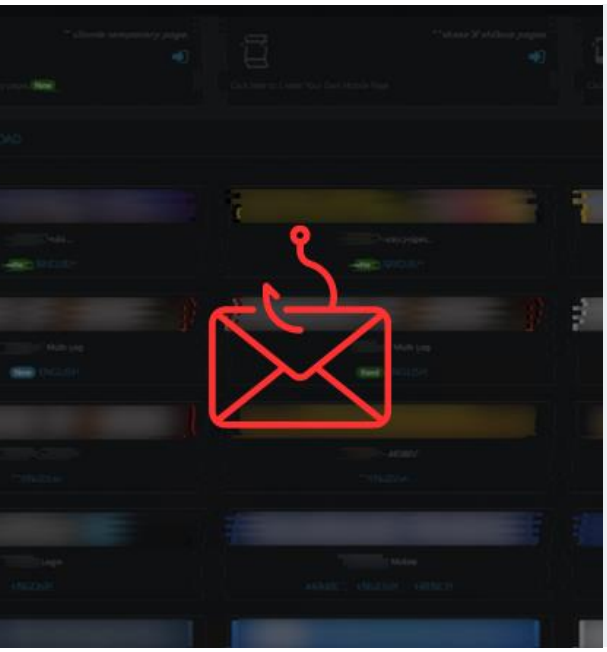
APT skupina Kimsuki kompromitovala systémy nemeckej spoločnosti

Severokorejská APT skupina KIMSUKI kompromitovala systémy nemeckej spoločnosti DIEHL DEFENCE, ktorá vyrába systémy protivzdušnej obrany IRIS-T dodávané aj Južnej Kórei. Skupina na prienik do systémov použila spear-phishingovú kampaň s tematikou pracovných ponúk, ktorá šírila škodlivé PDF dokumenty. Tento malvér im umožnil získať prístup k citlivým informáciám a potenciálne narušiť operácie spoločnosti. Útok je súčasťou širšej stratégie severokórejských útočníkov, ktorí sa často zameriavajú na zbrojárske spoločnosti a iné kritické infraštruktúry po celom svete.

Globálna malwarová kampaň zameraná na podnikové stránky Meta

Bezpečnostní výskumníci zverejnili informácie o rozsiahlej malwaretisement kampani, v rámci ktorej útočníci na šírenie a riadiacu komunikáciu malvéru SYS01STEALER zneužívajú kompromitované FACEBOOK kontá a reklamnú platformu META. Po kliknutí na reklamu skript exfiltruje údaje z prehliadača, získava kontrolu nad Facebook účtom obete a následne ju presmerováva na škodlivé stránky slúžiace pre stiahnutie škodlivých ZIP archívov so samotným malwarom. Zneužitie reklamných platforiem spoločnosti META a GOOGLE a taktiež rôznych služieb pre rozposielanie marketingových kampaní poskytuje útočníkovi mechanizmy pre jednoduchú distribúciu, cielenie a taktiež aj monitorovanie úspešnosti kampane.

VÝZNAMNÉ UDALOSTI VO SVETE



Phishingová platforma Sniper DZ a jej unikátne taktiky na útoky

Bezpečnostní výskumníci odhalili vyše 140 000 phishingových stránok, ktoré boli vytvorené prostredníctvom bezplatnej phishing-as-a-service služby SNIPER DZ. Phishing môže byť prevádzkovaný na proxy infraštruktúre predmetnej služby alebo vlastnom hostingu útočníka. Podľa informácií od bezpečnostných výskumníkov z UNIT42 sú exfiltrované dáta obetí preposielané aj samotným prevádzkovateľom služby. Sniper DZ má globálny dosah a jeho útoky boli zaznamenané v rôznych odvetviach, vrátane finančného sektora a vládnych organizácií. Základnom úspešnej ochrany pred týmto typom útoku je nasadenie viacfaktorovej autentifikácie a kontinuálne vzdelávanie zamestnancov o rizikách phishingu.

Zraniteľnosti v tlačovom subsystéme CUPS možno zneužiť na DDoS útoky

Bezpečnostní výskumníci zo spoločnosti AKAMAI odhalili, že nedávno opravené zraniteľnosti v tlačovom systéme CUPS možno zneužiť aj na realizáciu DDoS útokov s amplifikačným faktorom 600x. Pri zaslaní špeciálne vytvorených UDP paketov zraniteľné zariadenia generujú objemovo veľké IPP/HTTP požiadavky na zariadenia obete, čím dochádza k zahlteniu šírky pásma aj výpočtových zdrojov. Vládna jednotka CSIRT v súvislosti s uvedenými zraniteľnosťami zverejnila varovanie na svojej webovej stránke.

VÝZNAMNÉ UDALOSTI VO SVETE

- Ministerstvo spravodlivosti USA v spolupráci so spoločnosťou MICROSOFT zaistilo 107 domén ruskej štátom sponzorovanej skupiny COLDRIVER

- Platforma Telegram začala spolupracovať s orgánmi činnými v trestnom konaní a po doručení súdnej žiadosti zdieľať dáta o používateľoch.

- Anglický úrad pre jadrový dozor ONR udelil továrni na spracovanie jadrového odpadu SELLAFIELD pokutu vo výške 440 tisíc dolárov za nedostatočnú implementáciu kybernetickej bezpečnosti

- EURÓPSKY NAJVYŠŠÍ SÚD zakázal spoločnosti META využívanie osobných údajov získaných z platformy FACEBOOK na poskytovanie cielenej reklamy

- Spoločnosť CASIO sa stala obeťou útoku, v rámci ktorého útočníci prenikli do sieťovej infraštruktúry a spôsobili nedostupnosť viacerých služieb

- Ukrajinská polícia zadržala 28-ročného muža, ktorý prevádzkoval rozsiahlu VPN službu umožňujúcu prístup do ruského internetu

- Bezpečnostní výskumníci zverejnili analýzu Android malvéru TRICKMO, ktorý získava prihlasovacie údaje do bankových aplikácií a PIN kódy zariadení

- Výskumníci informovali o malwaretisement kampani, v rámci ktorej útočníci zneužívajú tzv. CLICKFIX techniku

- Spoločnosť MICROSOFT v produkte WINDOWS SERVER oficiálne ukončila podporu PPTP a L2TP/IPSEC protokolov pre vzdialený prístup a odporučila prechod na SSTP a IKEV2

- Spoločnosť CISCO pridala do zariadení CISCO ASA (Adaptive Security Appliance) a FTD (Firewall Threat Defense) nové funkcionality pre detekciu a mitigáciu brute-force a password spraying útokov

- Spoločnosť MICROSOFT zavádza dodatočnú ochranu MS EXCHANGE ONLINE voči TLS downgrade a man-in-the-middle útokom založenú na SMTP DANE s DNSSEC

- Spoločnosť META predstavila novú funkcionalitu aplikácie WHATSAPP, ktorá má zjednodušiť manažment kontaktných údajov a zvýšiť úroveň ich zabezpečenia.

- Účastníci hackerskej súťaže PWN2OWN IRELAND 2024 odhalili veľké množstvo zero-day zraniteľností v mobiloch, sieťových tlačiarňach a úložiskách

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v IDS/IPS Suricata

Vývojári IDS/IPS systému a sieťového analyzátora Suricata vydali aktualizáciu svojho produktu, ktorá opravuje šesť zraniteľností, z čoho tri sú označené ako kritické. Zraniteľnosti možno zneužiť na obídenie bezpečnostných mechanizmov, vzdialené vykonanie škodlivého kódu a zneprístupnenie služby.

Zraniteľnosť WordPress LiteSpeed Cache umožňuje stored XSS

Vývojári pluginu WordPress LiteSpeed Cache vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť súvisiacu s absentujúcou sanitizáciou parametrov z HTTP požiadaviek. Tieto plugin preberá a ukladá na administrátorskú stránku, čo vedie k možnosti vykonávať útoky typu stored XSS.

Zraniteľnosť Apache Avro umožňuje vykonávať kód

Systém pre serializáciu dát Apache Avro Java SDK kvôli chybe v spracovaní používateľských schém umožňuje útočníkom získať schopnosť vzdialeného vykonávania kódu.

Kritické a zero-day zraniteľnosti čipov Qualcomm

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte Expedition. Zraniteľnosti možno zneužiť na SQL injekciu, realizáciu XSS útokov, získanie neoprávneného prístupu k citlivým údajom a čítanie a zápis ľubovoľných súborov na súborovom systéme Expedition. Útočníci môžu získať schopnosť vzdialene vykonať škodlivý kód a získať úplnú kontrolu nad firewallmi s operačným systémom PAN-OS.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívaná RCE zraniteľnosť Firefox

Spoločnosť Mozilla opravila vo svojom prehliadači kritickú aktívne zneužívanú zraniteľnosť. Jej zneužitím získajú útočníci možnosť vzdialene vykonávať kód.

Kritické zraniteľnosti Palo Alto Networks Expedition

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produkte Expedition. Zraniteľnosti možno zneužiť na SQL injekciu, realizáciu XSS útokov, získanie neoprávneného prístupu k citlivým údajom a čítanie a zápis ľubovoľných súborov na súborovom systéme Expedition. Útočníci môžu získať schopnosť vzdialene vykonať škodlivý kód a získať úplnú kontrolu nad firewallmi s operačným systémom PAN-OS.

Microsoft Patch Tuesday opravuje 5 zero-day zraniteľností

Spoločnosť Microsoft v rámci októbrového Patch Tuesday vydala bezpečnostné aktualizácie svojich produktov, ktoré opravujú 118 zraniteľností, z toho 3 kritické, 5 zero-day a 2 aktívne zneužívané. Zero-day zraniteľnosti umožňujú vzdialené vykonanie kódu, obídenie bezpečnostných prvkov, eskaláciu privilégií a realizáciu útokov falšovaním rôznych prvkov.

Kritická zraniteľnosť GitLab umožňuje ľubovoľné spustenie CI/CD pipelinov

Spoločnosť GitLab vydala aktualizáciu, ktorá opravuje osem zraniteľností. Najzávažnejšie umožňujú vzdialeným útočníkom spustiť CI/CD pipeline na ľubovoľnej vetve repozitára a vykonávať škodlivý kód. Medzi ďalšie závažné zraniteľnosti patrí možnosť realizácie SSRF a XSS útokov, zneprístupnenie služieb a neoprávnený prístup k citlivým údajom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v produkte Trend Micro Cloud Edge

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Cloud Edge. Zraniteľnosť o označením CVE-2024-48904 možno zneužiť na vzdialené vykonanie škodlivého kódu.

Vysoko závažná zraniteľnosť v produkte VMware HCX

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v produkte VMware HCX. CVE-2024-38814 možno prostredníctvom SQL injekcie zneužiť na vzdialené vykonanie kódu.

Zraniteľnosti F5 BIG-IP a BIG-IQ

Spoločnosť F5 vydala bezpečnostné aktualizácie, ktoré opravujú 2 zraniteľnosti v F5 BIG-IP a F5 BIG-IQ. Vzdialený autentifikovaný útočník ich dokáže zneužiť na zvýšenie privilégií, vykonávanie kódu JavaScript a prevzatie kontroly nad zariadením.

Závažná zraniteľnosť Windows Registry

Microsoft opravil vysoko závažnú zraniteľnosť vo Windows Registry, ktorá umožňuje eskaláciu oprávnení na serveri na úroveň SYSTEM. Zraniteľnosť bola opravená v rámci októbrového balíka Microsoft Patch Tuesday.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Potenciálna zraniteľnosť frameworku Nette umožňujúca SQL injection

Bezpečnostní analytici CSIRT.SK objavili potenciálnu zraniteľnosť vo webovom frameworku Nette, ktorá umožňuje vykonávať útoky typu SQL injection. Zraniteľnosť sa nachádza v knižnici Database a súvisí s absenciou ošetrovania používateľských vstupov, ktoré preberá funkcia where($by).

Novú kritickú zraniteľnosť FortiManager aktívne zneužívajú na vykonávanie kódu

Spoločnosť Fortinet opravila kritickú aktívne zneužívanú zero-day zraniteľnosť v produkte FortiManager. CVE-2024-47575 spočíva v chýbajúcej autentifikácii pre prístup ku rozhraniu API, ktoré umožňuje vykonávanie príkazov, prístup k citlivým údajom a prevzatie kontroly nad FortiManager a v ňom spravovanými zariadeniami.

Kritické zraniteľnosti produktov Cisco

Spoločnosť Cisco opravila kritické zraniteľnosti vo viacerých svojich produktoch. Zraniteľnosti Cisco Secure Firewall Management Center a Adaptive Security Appliance umožňujú vykonávanie ľubovoľných systémových príkazov s oprávneniami používateľa root. Zraniteľnosť Firepower Threat Defense súvisí s prítomnosťou prihlasovacích údajov v kóde systému a umožňuje tak neoprávnený prístup do systému.

NVIDIA opravila závažné zraniteľnosti ovládačov

Spoločnosť nVidia vydala bezpečnostné aktualizácie, ktoré opravujú viacero vysoko závažných zraniteľností v ovládačoch grafických kariet. Najzávažnejšiu zraniteľnosť s označením CVE-2024-0126 by lokálny autentifikovaný útočník mohol zneužiť na eskaláciu privilégií a vykonanie škodlivého kódu. Ostatné zraniteľnosti možno zneužiť na vykonanie kódu, zneprístupnenie služby, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v produktoch QNAP HBS 3 Hybrid Backup Sync a SMB Service

Spoločnosť QNAP vydala bezpečnostné aktualizácie svojho nástroja pre zálohovanie a obnovu dát HBS 3 (HYBRID BACKUP SYNC), ktoré opravujú kritickú zero-day zraniteľnosť. CVE-2024-50388 možno zneužiť na vzdialené vykonanie kódu. HBS 3 je používaný v rámci sieťových úložísk QNAP NAS s operačnými systémami QTS a QuTS hero. Aktualizácie opravujú tiež kritickú zero-day zraniteľnosť SMB Service, ktorá umožňuje útoky typu SQL injection a získanie kontroly nad zariadením.

Kritická zraniteľnosť Spring WebFlux

Spoločnosť Broadcom vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť vo webovom frameworku Spring WebFlux. Bližšie nešpecifikovanú zraniteľnosť s označením CVE-2024-38821 by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie bezpečnostných mechanizmov a narušenie dôvernosti a integrity systému.

Protect AI: Októbrové zraniteľnosti v modeloch AI

Protect AI's huntr je prvý program odmeňovania za nájdenie zraniteľností v oblasti AI/ML na svete. Októbrová správa tejto iniciatívy informuje o 34 objavených zraniteľnostiach, z toho sú 3 kritické. Najzávažnejšie chyby umožňujú vzdialené vykonávanie kódu, prístup ku chráneným zdrojom a únik citlivých informácií.

MESAČNÍK ZRANITEĽNOSTÍ OKTÓBER 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
   - Lunary, gaizhenbiao/chuanhuchatgpt, Mudler/localai
   - Spring WebFlux
   - QNAP HBS 3 Hybrid Backup Sync, QNAP SMB Service
   - Ovládače grafických kariet NVIDIA GeForce, NVIDIA RTX, Quadro, NVS, Tesla, vGPU a Cloud Gaming
   - Cisco Secure Firewall Management Center (FMC), Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD)
   - Fortinet FortiManager, FortiManager Cloud
   - Nette Framework
   - Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
   - F5 BIG-IP (všetky moduly), BIG-IQ
   - VMware HCX
   - Trend Micro Cloud Edge
   - GitLab Community Edition (CE), GitLab Enterprise Edition (EE)
   - .NET, Azure CLIAzure Monitor Agent, Azure Service Connector, Azure Service Fabric, Azure Stack HCI, CBL Mariner, DeepSpeed, Microsoft .NET Framework, Microsoft 365 Apps for Enterprise, Microsoft Configuration Manager, Microsoft Copilot Studio, Microsoft Defender for Endpoint for Linux, Microsoft Edge (Chromium-based), Microsoft Excel, Microsoft Office, Microsoft Outlook for Android, Microsoft SharePoint, Microsoft Visual Studio, Power BI Report Server, Remote Desktop client for Windows Desktop, Visual C++ Redistributable Installer, Visual Studio CodeWindows 10 for 32-bit Systems, Windows, Windows Server
   - Palo Alto Networks Expedition
   - Firefox, Firefox ESR

- Qualcomm Digital Signal Processor (DSP), Qualcomm WLAN Resource Manager
- Apache Avro Java SDK
- WordPress LiteSpeed Cache
- IDS/IPS Suricata

https://csirt.sk/posts/1631.html