CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

NOVEMBER 2024

TLP: CLEAR

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CSIRT.SK

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

1 Zraniteľnosť v knižnici Querydsl možno zneužiť na SQL/HQL

Bezpečnostní analytici CSIRT.SK objavili novú zraniteľnosť v Java knižnici Querydsl, ktorá umožňuje vykonávať útoky typu SQL/HQL injection.

2 Čínska skupina SILKSPECTER vytvorila rozsiahlu sieť falošných

Čínska finančne motivovaná skupina SILKSPECTER prevádzkuje rozsiahlu sieť falošných online obchodov, ktorej cieľom je získavanie platobných údajov a telefónnych čísel obetí v USA a Európe.

3 Útočníci používajú novú metódu pre zneužitie bankových údajov

Spoločnosť THREATFABRIC zachytila nový typ útoku pre zneužitie bankových údajov, ktorý spočíva v replikácii NFC signálov a využití organizovanej siete subjektov pre interakciu s PoS terminálmi.

4 Čínska skupina SALT TYPHOON prenikla do systémov telekomunikačných operátorov v USA

Hackerskej skupine SALT TYPHOON sa v rámci útokov cielených na telekomunikačných operátorov v USA podarilo získať prístup k privátnej komunikácii niektorých vládnych predstaviteľov.

5 Zneužitie platforiem Spotify a Amazon na promovanie škodlivého obsahu

Aktéri na promovanie škodlivého obsahu začali aktívne zneužívať rôzne funkcie platforiem Spotify a Amazon, ktorých obsah je indexovaný internetovými vyhľadávačmi.

6 Zneužitie chyby v Microsoft 365 Admin Portal na rozposielanie sextortion správ

Útočníci v rámci rozsiahlej sextortion kampane na obchádzanie bezpečnostných mechanizmov pre detekciu podozrivej pošty zneužívajú chybu v Microsoft 365 Admin Portal.

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.

Najzávažnejšou phishingovou kampaňou, ktorú jednotka v posledných mesiacoch riešila, boli podvodné spear-phishingové (cielené) e-maily odoslané z falošnej domény „vladagov.sk“. V podpise bolo uvedené skutočné meno IT administrátora Úradu vlády SR. Podľa znenia správ bolo cieľom útočníkov získať prihlasovacie údaje do e-mailových schránok zamestnancov ÚV SR. Útok realizovali prostredníctvom podvrhnutých generických adries s takmer identickou doménou skutočnej vládnej: “oznamy[@]goverment[.]sk”, „oznamy[@]vladagov[.]sk“. V súvislosti s „*@vladagov[.]sk” došlo k interakcii dvoch zamestnancov, a to vyplnením svojich údajov do podvrhnutého webového formulára.

Ani tento mesiac sa nevyhol e-mailovým vyhrážkam bombovými útokmi na organizácie v konštituencii VJ CSIRT. Opäť boli medzi nimi aj školy. E-maily mali viacero foriem, no najčastejšie obsahovali výhražnú správu v mene Islamského štátu o uložení výbušniny v areáli organizácie. Jednotka si vyžiadala originálne e-mailové správy za účelom analýzy. Pri prípade bola súčinná s Políciou SR a jednotkou SK-CERT.

Organizácia v konštituencii CSIRT.SK nahlásila podozrivé aktivity pri prihlasovaní do platformy Microsoft 365 s vysokou koncentráciou. Aktivity prebiehali z IP adries geolokalizovaných v Ruskej federácii a trvali niekoľko dní. Pokusy o prihlásenie k účtom zamestnancov neboli úspešné. Pozorované IP adresy boli v rámci siete Govnet zablokované.

CSIRT.SK sa v novembri stretol aj s prípadom ransomvérového útoku (malvér z rodiny LYNX) na infraštruktúru organizácie v konštituencii jednotky. CSIRT.SK poskytol informácie tímu SK-CERT a ponúkol súčinnosť pri riešení incidentu.

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, ktorú monitoruje modul Domino.

V novembri CSIRT.SK plošne varoval svoju konštituenciu ohľadom

zraniteľností CVE-2024-11068 v routroch D-Link DSL6740C s ukončenou technickou podporou, o ktorých písal aj na svojej webstránke. Najzávažnejšiu z nich možno zneužiť na získanie úplnej kontroly na zraniteľným zariadením.

CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej

bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných

škôl. V novembri prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov

Kancelárie najvyššieho súdu SR. Diskusných prednášok pre študentov sa zúčastnili študenti nasledujúcich škôl:

- SPŠ Chemická, Bratislava
- SOŠ Masmediálnych a informačných služieb, Bratislava
- Adlerka- SPŠ Elektrotechnická, Bratislava
- SPŠ Dopravná, Trnava
- SOŠ pedagogická, Modra
- Gymnázium sv. Košických mučeníkov, Košice
- OA Watsonova, Košice
- SOŠ Beauty Služieb, Košice
- Spojená škola internátna Prakovce
- Gymnázium Krompachy

Členovia tímu CSIRT.SK sa v novembri na základe pozvania zúčastnili Kongresu Asociácie stredných odborných škôl Slovenka, ktorý sa konal v Hornom Smokovci. Zúčastneným riaditeľom škôl prezentovali služby VJ CSIRT, relevantné pre školy. Konkrétne sa venovali poskytovaniu pomoci pri riešení kybernetických bezpečnostných incidentov, preventívnemu skenovaniu a reportovaniu zraniteľností systémom Achilles a vzdelávacím aktivitám pre študentov a učiteľov v oblasti kybernetickej bezpečnosti.

V rámci tréningu svojich zručností sa členovia VJ CSIRT zúčastnili súťaže Capture the Flag zameraného na platformu XDR spoločnosti Trend Micro. Súťaž organizovala spoločnosť Alanata. Členovia tímu CSIRT.SK v nej obsadili prvé tri miesta.

VÝZNAMNÉ UDALOSTI VO SVETE

Vládna jednotka CSIRT objavila zraniteľnosť v knižnici Querydsl a OpenFeign Querydsl

Bezpečnostní analytici CSIRT.SK objavili novú zraniteľnosť v Java knižnici Querydsl a OpenFeign Querydsl, ktorú možno zneužiť na realizáciu SQL/HQL injekcie. Zraniteľnosť s identifikátorom CVE-2024-49203 sa nachádza vo funkcii orderBy slúžiacej pre usporiadanie výsledkov databázových dopytov a spočíva v chýbajúcom overovaní používateľských vstupov. Informácie o zraniteľnosti boli v rámci procesu zodpovedného nahlasovania zraniteľností zdieľané s autormi knižnice. Pokiaľ pri vývoji webových aplikácií v programovacom jazyku Java využívate zraniteľnú metódu orderBy tejto knižnice, odporúčame implementovať dodatočné overovanie používateľských vstupov podľa best practice pre bezpečný vývoj softvéru.

Čínska hackerská skupina Storm-0940 na prienik do systémov zneužíva botnet QUAD7

Spoločnosť MICROSOFT varovala, že čínski hackeri na prienik do systémov prostredníctvom rozsiahlych password-spraying útokov zneužívajú QUAD7 botnet, ktorý pozostáva z kompromitovaných SOHO routerov. Útočníci sa pri maskovaní svojej aktivity spoliehajú na minimalizáciu počtu súvislých pokusov o prihlásenie za isté časové obdobie, pričom v 80 percentách analyzovaných prípadov sa dokonca jednalo o maximálne jeden pokus za deň. Po prieniku do systémov útočníci skúmajú sieť, vytvárajú perzistentný prístup a prostredníctvom rôznych nástrojov a malvéru exfiltrujú prihlasovacie údaje.

Útočníci zneužívajú Ethereum smart kontrakty v rámci riadiacej infraštruktúry malvéru

Bezpečnostní výskumníci identifikovali približne 300 NPM knižníc imitujúcich názvy legitímnych knižníc, ktoré sú zneužívané v rámci rozsiahlej malwaretisement kampane. Malvér na distribúciu IP adresy riadiaceho servera využíva Ethereum smart kontrakty, s ktorými interaguje prostredníctvom knižnice ether.js. Obfuskovaný JavaScript na základe typu operačného systému obete sťahuje príslušný malvér, ktorý sa po vytvorení perzistentného prístupu k zariadeniu zameriava na exfiltráciu citlivých údajov. Využitie smart kontraktov v rámci riadiacej infraštruktúry malvéru je pomerne ojedinelé. Uvedená kampaň zdôrazňuje potrebu prísnej kontroly balíkov a nástrojov počas celého životného cyklu vývoja softvéru.

VÝZNAMNÉ UDALOSTI VO SVETE

Aktívne zneužitie post-exploitačného frameworku Winos4.0 v rámci útokov

Bezpečnostní výskumníci počas analýzy útokov zameraných na čínsky hovoriacu hráčsku komunitu zaznamenali nárast využitia post-exploitačného frameworku WINOS4.0. Jedná sa o plnohodnotnú alternatívu nástrojov COBALT STRIKE a SLIVER, ktorá obsahuje funkcie pre zber informácií o infikovanom systéme, kontrolu prítomnosti antivírusových a bezpečnostných riešení, udržiavanie permanentného spojenia s riadiacim serverom útočníka (tzv. C2 server), zber a následnú exfiltráciu citlivých údajov. Analytické zistenia výskumníkov bezpečnostná komunita využije na prípravu nových metód pre detekciu tohto frameworku, ktoré možno použiť v rámci prevencie a pri riešení kybernetických bezpečnostných incidentov.

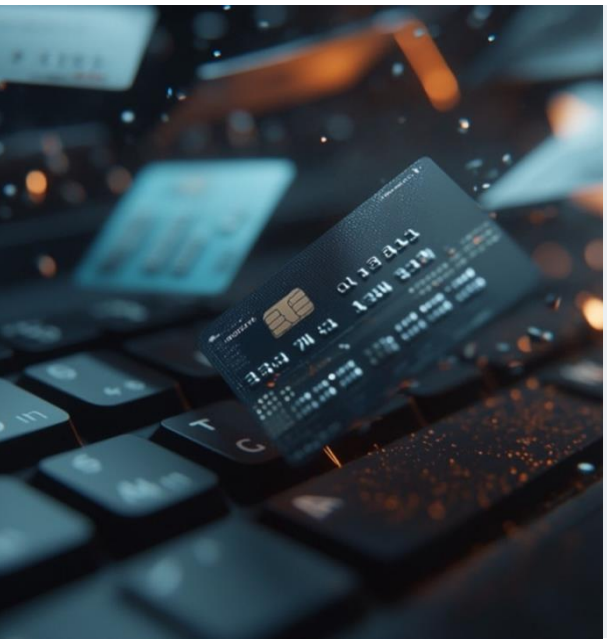
Aktívne zneužitie metódy „ZIP CONCATENATION“ na šírenie malvéru

Bezpečnostní výskumníci zverejnili informácie o malwaretisement kampani, v rámci ktorej útočníci na šírenie malvéru aktívne zneužívajú metódu „ZIP concatenation“. Technika spočíva vo vytvorení viacerých ZIP súborov, ich následnom spojení do jedného archívu a zneužití rozdielnych prístupov ZIP parserov a archivačných aplikácií pri ich spracovaní. Výskumníci testovali rozdiely pri spracovaní archívov vytvorených touto metódou v rámci aplikácií 7ZIP, WINRAR a WINDOWS FILE EXPLORER. Napriek tomu, že sa jedná o už známu metódu pre distribúciu malvéru, stále ju možno efektívne zneužiť na obídenie rôznych detekčných mechanizmov v rámci prvkov antivírusovej ochrany.

Nový ransomvér YMIR napadá zariadenia infikované stealerom RUSTYSTEALER

Bezpečnostní výskumníci zverejnili informácie o novom ransomvére YMIR, ktorý sa šíri na zariadeniach infikovaných malvérom RUSTYSTEALER. Technická analýza odhalila, že Ymir beží priamo v operačnej pamäti zariadenia (tzv. fileless malvér), jeho zdrojový kód obsahuje komentáre v africkom jazyku Lingala, vytvára ransomnote v podobe PDF dokumentov a ponúka veľa rozšírení a režimov konfigurácie. Napriek existencii funkcií pre komunikáciu s riadiacim serverom útočníka ešte skupina nemá zriadenú leakpage slúžiacu na zverejnenie exfiltrovaných údajov. V rámci analyzovaných incidentov došlo k nasadeniu ransomvéru približne dva dni po prvotnej infekcii stealerom. Analyzované incidenty poukazujú na pokračujúci trend prehlbovania vzájomnej spolupráce medzi kyberkriminálnikmi.

VÝZNAMNÉ UDALOSTI VO SVETE

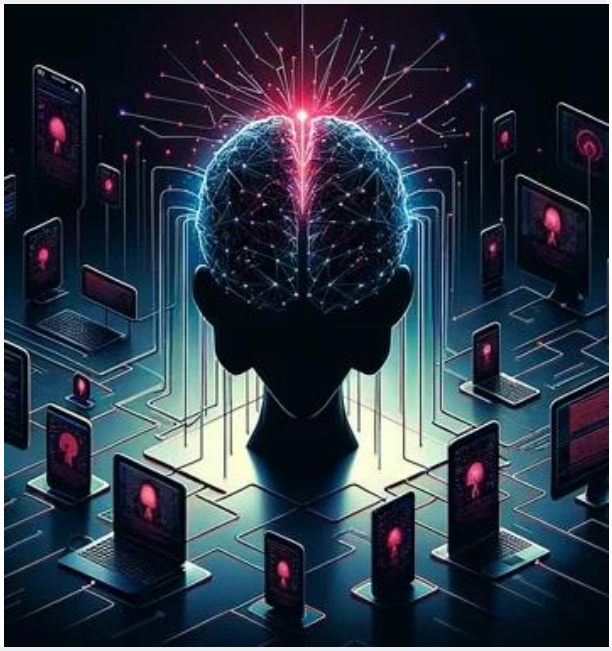


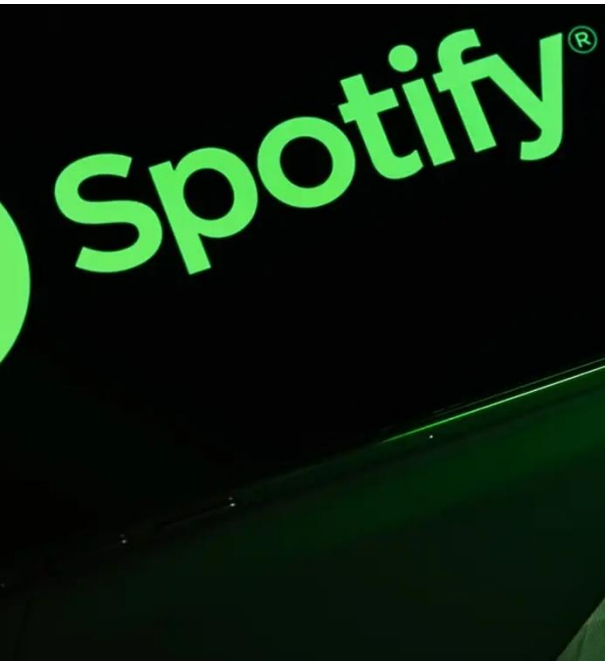
Čínska skupina Silkspecter vytvorila rozsiahlu sieť falošných e-shopov

Bezpečnostní výskumníci zverejnili informácie o sieti falošných online obchodov čínskej finančne motivovanej skupiny SILKSPECTER, ktorej cieľom je získanie platobných údajov a telefónnych čísel obetí v USA a Európe. Podvodné stránky zneužívajú identitu populárnych značiek a tematiku Black Friday zliav. Po technickej stránke integrujú platobnú bránu STRIPE a na monitorovanie úspešnosti zneužívajú populárne tracking pixely OpenRelay, TikTok Pixel a Meta Pixel. Útočníci okrem získania finančných prostriedkov zo samotných platieb zadané údaje exfiltrujú za účelom ich ďalšieho zneužitia alebo predaja. Základné odporúčania pre rozpoznanie podozrivých e-shopov môžete nájsť aj na stránke NBÚ.

Malwaretisement kampaň s tematikou AI aplikácií pre generovanie obrazu a videa

Bezpečnostní výskumníci zachytili rozsiahlu malwaretisement kampaň s tematikou AI aplikácií pre generovanie obrazu a videa, ktorá zariadenia obetí infikuje infostealermi LUMMA STEALER (platforma Windows) a AMOS (platforma macOS). Primárnym cieľom uvedených malvérov je získanie a exfiltrácia kryptopeňaženiek a citlivých údajov. Kampaň sa šíri prostredníctvom príspevkov a reklamy na sociálnej sieti X. Vzhľadom na pokračujúci trend rozvoja rôznych nástrojov umelej inteligencie a popularitu sociálnych sietí sa jedná o účinný vektor distribúcie malvéru a následného prieniku do systémov. Z dlhodobého hľadiska Vládna jednotka CSIRT zo strany útočníkov deteguje narastajúci trend zneužívania platenej reklamy na promovanie škodlivého obsahu.





Zneužitie hudobnej platformy Spotify na promovanie škodlivého obsahu

Bezpečnostní výskumníci zachytili malwaretisement kampaň, v rámci ktorej útočníci na promovanie škodlivého obsahu zneužívajú playlisty, podcasty a komentáre na platforme SPOTIFY. Vzhľadom na popularitu platformy totiž dochádza k indexovaniu jej obsahu internetovými vyhľadávačmi, čím navyše útočníci dokážu ovplyvniť aj SEO (Search Engine Optimization) svojich stránok. Okrem playlistov a komentáro dochádza aj k zneužitiu podcastov so syntetizovaným hlasom, ktoré taktiež navádzajú ku stiahnutiu obsahu. Spotify síce predmetný obsah po nahlásení porušenia svojich licenčných podmienok vymazáva, ale incident poukazuje na absenciu automatických mechanizmov moderovania a unikátny vektor šírenia škodlivého obsahu.

VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci zneužili chybu v Microsoft 365 Admin Portal na rozposielanie sextortion správ

Bezpečnostní výskumníci zachytili masívnu sextortion kampaň, v rámci ktorej útočníci na rozposielanie e-mailových správ zneužívajú MICROSOFT 365 ADMIN PORTAL, čo im umožňuje obísť bezpečnostné mechanizmy pre detekciu podozrivej pošty. Komponent Message Center v rámci administratívneho rozhrania slúži na zobrazenie správ, noviniek a upozornení od spoločnosti Microsoft. Tie možno prostredníctvom funkcie SHARE preposlať na 2 ľubovoľné e-mailové adresy aj so sprievodným komentárom, do ktorého je umiestňovaná výhražná správa. Útočníci jednoduchou editáciou HTML kódu príslušných komponentov obišli maximálny 1000 znakový limit dĺžky sprievodnej správy a celý proces zneužitia zraniteľnosti zautomatizovali. Spoločnosť Microsoft situáciu skúma a plánuje implementovať opatrenia pre mitigáciu chyby. Incident poukazuje na vynaliezavosť útočníkov pri hľadaní nových metód pre distribúciu phishingového a škodlivého obsahu.

Nová metóda Ghost Tap umožňuje výber peňazí pomocou replikácie NFC signálov

Bezpečnostní výskumníci zo spoločnosti THREATFABRIC zachytili nový typ útoku pre zneužitie bankových údajov, ktorý spočíva v replikácii NFC signálov. Nová metóda s označením GHOST TAP spočíva v pridaní odcudzených kariet do mobilných platobných aplikácií APPLE PAY a GOOGLE PAY na zariadení útočníka, preposlanie NFC signálu z aplikácie pripravenej na platbu na centrálny relay server útočníka. Zo serveru sú ďalej preposielané na organizovanú sieť kriminálnikov (tzv. money mules), ktorých úlohou je fyzicky dáta zneužiť interakciou s PoS terminálmi, čo značne komplikuje identifikáciu samotného hlavného aktéra a súvisiacej infraštruktúry. Metódu je možné detegovať zachytením platieb z rôznych miest, medzi ktorými by sa človek fyzicky nedokázal za uvedený čas presunúť. Podobnú metódu používal malvér NGATE, ktorého činnosť v auguste 2024 zdokumentovala spoločnosť ESET.

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CSIRT.SK

VÝZNAMNÉ UDALOSTI VO SVETE

Zneužitie služieb spoločnosti Amazon na promovanie škodlivého obsahu

Bezpečnostní výskumníci zachytili malwaretisement kampaň, v rámci ktorej útočníci škodlivý obsah promujú prostredníctvom služieb AMAZON, AMAZON MUSIC a AUDIBLE. Nakoľko sú uvedené služby indexované aj internetovými vyhľadávačmi, aktérom to umožňuje vykonávať tzv. SEO poisoning na promovanie rôznych stránok s tematikou obchodovania, telegramových kanálov a iných odkazov slúžiacich na sťahovanie pirátskych verzií populárnych softvérov. V novembri 2024 CSIRT.SK zachytil informácie o podobnej metóde, ktorá zneužívala playlisty a podcasty na platforme Spotify. Obe kampane poukazujú, že útočníci aktívne hľadajú nové metódy promovania a distribúcie obsahu a taktiež problémy s moderovaním obsahu na online platformách.

Čínska skupina Salt Typhoon prenikla do systémov telekomunikačných operátorov v USA

Spoločnosť TREND MICRO zverejnila informácie o útokoch čínskej štátom sponzorovanej skupiny SALT TYPHOON cielených na telekomunikačných operátorov v USA, v rámci ktorej sa jej podarilo získať prístup k privátnej komunikácii niektorých vládnych predstaviteľov v USA. Skupina na prvotný prienik do systémov primárne zneužíva bezpečnostné zraniteľnosti v produktoch Ivanti Connect Secure, Fortinet FortiClient EMS, Sophos Firewall a Microsoft Exchange. Systémy infikujú backdoormi, rootkitom DEMODEX, malware dropperom SHADOWPAD a využívajú aj tunelovací nástroj, reverzné proxy a komerčný nástroj COBALT STRIKE. Na základe nedávnych incidentov a TTP sa jedná o jedného z najagresívnejších a najúspešnejších čínskych aktérov v súčasnosti.

Výskumníci objavili nový malvér zneužívajúci herný engine Godot

Spoločnosť CHECKPOINT zverejnila analýzu malware loadera GODLOADER, ktorý zneužíva funkcionality herného enginu GODOT. Nakoľko sa jedná o multiplatformové prostredie, umožňuje cielenie útokov na rôzne operačné systémy a jeho interný skriptovací jazyk GDScript možno prostredníctvom špeciálne vytvorených .PCK súborov zneužiť na obídenie detekčných mechanizmov. Primárnym cieľom malvéru je exfiltrácia citlivých údajov a ťažba kryptomien prostredníctvom nástroja XMRIG, ktorého konfigurácia sa načítava zo služby PASTEBIN. GodLoader je aktívne zneužívaný minimálne od 29. júna 2024 a na jeho šírenie útočníci zneužívajú malware-distribution-as-a-service platformu STARGAZERS GHOST NETWORK, ktorá zneužíva rozsiahlu sieť GITHUB účtov a repozitárov.

VÝZNAMNÉ UDALOSTI VO SVETE

Ruská skupina Romcom v rámci kybernetických útokov kombinuje zero-day zraniteľnosti

Ruská hackerská skupina ROMCOM na šírenie backdoorov v rámci útokov na ciele v Európe a severnej Amerike zneužíva zero day zraniteľnosti v prehliadači Mozilla Firefox a komponente Windows Task Scheduler. Zraniteľnosť CVE-2024-9680 vo Firefox umožňuje vykonanie kódu v sandboxovom prostredí prehliadača a CVE-2024-49039 vo Windows Task Scheduler možno zneužiť na eskaláciu privilégií a vykonanie kódu mimo sandboxu prehliadača. Podľa spoločnosti ESET bola kampaň cielená na používateľov prehliadačov Firefox a Tor Browser. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí navštíviť špeciálne vytvorenú stránku. V rámci subjektov patriacich do konštituencie CSIRT.SK neboli zaznamenané žiadne súvisiace incidenty. Pokročilí útočníci sú schopní kombináciou zraniteľností rôznej závažnosti a v rôznych softvéroch vytvoriť efektívne metódy prieniku do systémov.

Supply chain útok prostredníctvom NPM knižnice implementujúcej XML-RPC

Bezpečnostní výskumníci zo spoločnosti CHECKMARX odhalili supply chain útok prostredníctvom NPM knižnice @0XENGINE/XMLRPC, do ktorej bol pridaný škodlivý kód slúžiaci pre exfiltráciu citlivých údajov prostredníctvom služieb Dropbox a file.io a ťažbu kryptomeny Monero pomocou nástroja XMRIG. Predmetná knižnica bola vytvorená 2. októbra 2023 ako implementácia XML-RPC servera a klienta pre Node.js a škodlivé časti sú v zdrojovom kóde prítomné od verzie 1.3.4. Na samotné šírenie okrem NPM útočníci vytvorili aj GitHub repozitár projektu, ktorý obsahoval skryté závislosti na túto knižnicu. Incident poukazuje na nebezpečenstvo supply chain útokov na rôzne knižnice programovacích jazykov, ku ktorým môže dôjsť následkom kompromitácie systémov vývojárov alebo sa jedná o dlhodobú a plánovanú aktivitu zo strany útočníka.

VÝZNAMNÉ UDALOSTI VO SVETE

- Útočníci na zariadeniach s operačným systémom WINDOWS vytvárajú virtuálne stroje so zabudovaným backdoorom

- Útočník vystupujúci pod aliasom GREP prenikol do vývojovej platformy spoločnosti SCHNEIDER ELECTRIC a exfiltroval približne 40 GB dát z JIRA servera

- Princípom CLICKFIX útokov je presvedčiť obeť, aby manuálne skopírovala a spustila škodlivé skripty

- Malwaretisement kampaň severokórejskej skupiny BLUENOROFF sa zameriava na subjekty pôsobiace v oblasti obchodovania s kryptomenami

- Najnovšia verzia mobilnej aplikácie GOOGLE SEARCH pri využití funkcie pre zdieľanie URL generuje odkazy v tvare "search.app?link=URL"

- OČTK identifikovali novú bezpečnostnú funkciu iOS 18.1, ktorá zapnuté zariadenia pri dlhej neaktivite reštartuje, čím komplikuje ich forenznú analýzu v rámci vyšetrovania

- Útočníci zneužívajú možnosti obrazového formátu SVG na zobrazenie phishingových formulárov, šírenie malvéru a maskovanie svojej činnosti

- Chybu v logovacom mechanizme VPN serverov od spoločnosti FORTINET možno zneužiť na maskovanie úspešnosti brute-force útokov

- Spoločnosť MICROSOFT zaistila 240 škodlivých domén vytvorených prostredníctvom phishing-as-a-service platformy ONNX

- Bezpečnostní výskumníci z INSIKT GROUP zverejnili informácie o malwaretisement kampani ruských aktérov s možným prepojením na APT28

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť WordPress pluginu LiteSpeed Cache umožňuje získanie administrátorského prístupu

Vývojári populárneho pluginu WordPress LiteSpeed Cache vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú bezpečnostnú zraniteľnosť. CVE-2024-50550 možno zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad systémom.

Kritická zraniteľnosť QNAP QuRouter

Spoločnosť QNAP vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zero-day zraniteľnosť vo svojom operačnom systéme QuRouter. Bližšie nešpecifikovanú zraniteľnosť s označením CVE-2024-50389 možno zneužiť na získanie úplnej kontroly nad zariadením. Informácie o druhu zraniteľnosti neboli zverejnené.

Kritická zraniteľnosť v produkte Cisco Unified Industrial Wireless Software

Spoločnosť Cisco vydala bezpečnostné aktualizácie svojho produktu Cisco Unified Industrial Wireless Software, ktoré opravujú kritickú zraniteľnosť. Produkt je využívaný v rámci URWB (Ultra Reliable Wireless Backhaul) prístupových bodov určených pre priemyselné siete. CVE-2024-20418 možno zneužiť na vzdialené vykonanie príkazov.

Zraniteľnosť v SQLite objavil model AI od Google

Tím Google Project Zero testoval využitie modelu umelej inteligencie Big Sleep pri hľadaní zraniteľností v známych open source produktoch. Model úspešne objavil zraniteľnosť v SQLite, ktorú neodhalili fuzzingové nástroje. Zraniteľnosť súvisí s podtečením medzipamäte zásobníka, čo môže viesť k schopnosti zapisovať na halde mimo povolené hodnoty.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v prístupových bodoch od HPE Aruba Networking

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností v operačných systémoch Instant AOS-8 a AOS-10 používaných v prístupových bodoch Aruba Series, z čoho 2 sú označené ako kritické. Zraniteľnosti CVE-2024-42509 a CVE-2024-47460 možno zneužiť na injekciu príkazov a vzdialené vykonanie škodlivého kódu.

Zraniteľnosť vo Veeam Backup Enterprise Manager možno zneužiť na obídenie mechanizmov autentifikácie

Spoločnosť Veeam vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v produkte Veeam Backup Enterprise Manager (VBEM). Zraniteľnosť CVE-2024-40715 možno zneužiť na obídenie mechanizmov autentifikácie.

Kritické bezpečnostné zraniteľnosti v produktoch Ivanti EPM, ICS a IPS

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 v routroch D-Link DSL6740C s ukončenou technickou podporou

Bezpečnostní výskumníci zverejnili informácie o 7 zraniteľnostiach routrov D-LINK DSL6740C, z ktorých jedna je označená ako kritická. Kritickú zraniteľnosť CVE-2024-11068 možno zneužiť na získanie úplnej kontroly na zariadením. Ostatné zraniteľnosti možno zneužiť na injekciu príkazov a získanie neoprávneného prístupu k citlivým údajom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Bridge, Audition, After Effects, Substance 3D Painter, Illustrator, InDesign, Photoshop a Commerce, ktoré opravujú 48 zraniteľností, z čoho 28 sú označené ako kritické. Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu.

Microsoft v rámci novembrového Patch Tuesday opravil 4 kritické zraniteľnosti

Spoločnosť Microsoft vydala v novembri 2024 balík opráv pre portfólio svojich produktov opravujúci 89 zraniteľností, z ktorých 52 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú vo frameworku .NET, produkte Visual Studio, komponentoch Windows VMSwitch a Window Kerberos a online platforme airlift.microsoft.com a možno ich zneužiť na eskaláciu privilégií a vzdialené vykonanie škodlivého kódu.

Aktívne zneužívaná kritická zraniteľnosť Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala varovanie ohľadom bližšie nešpecifikovanej kritickej zraniteľnosti v manažmentovom rozhraní firewallov, ktorá umožňuje vzdialené vykonávanie príkazov. Zraniteľnosť je aktívne zneužívaná a existuje na ňu verejne dostupný exploit.

Závažná zraniteľnosť PostgreSQL umožňuje vykonávať kód

V PostgreSQL bola opravená vysoko závažná zraniteľnosť súvisiaca s nevhodnou kontrolou premenných prostredia v PL/Perl. Jej zneužitím môže útočník získať schopnosť vykonávať ľubovoľný kód, získať citlivé informácie, alebo vykonať inú činnosť v závislosti napríklad od zneužitej premennej.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť modulu WordPress Really Simple Security

Vývojári modulu WordPress Really Simple Security opravili kritickú zraniteľnosť, ktorá umožňuje neprihlásenému útočníkovi získať neoprávnený prístup do zraniteľného systému ako ľubovoľný používateľ, vrátane administrátora.

Aktívne zneužívaná kritická zraniteľnosť zariadení GeoVision

Viacero produktov spoločnosti GeoVision s ukončenou podporou zneužívajú útočníci pre variant botnetu MIRAI. Infekcia prebieha po zneužití kritickej zraniteľnosti, ktorá umožňuje vykonávanie systémových príkazov bez potreby autentifikácie.

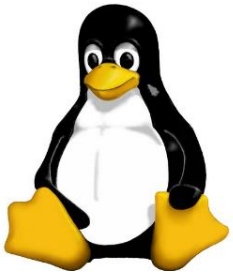
Zraniteľnosť knižnice Querydsl a OpenFeign Querydsl umožňujúca SQL/HQL injection

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť CVE-2024-49203 v Java knižnici Querydsl a OpenFeign Querydsl, ktorá umožňuje vykonávať útoky typu SQL/HQL injection.

Aktívne zneužívané zero-day zraniteľnosti v operačných systémoch macOS, iOS, iPadOS a visionOS a prehliadači Safari

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré opravujú 2 aktívne zneužívané zero-day zraniteľnosti v komponentoch operačných systémov macOS, iOS, iPadOS a visionOS a internetovom prehliadači Safari. CVE-2024-44308 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a CVE-2024-44309 na realizáciu XSS útokov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV



Kritická zraniteľnosť v routroch D-Link s ukončenou technickou podporou

Spoločnosť D-Link varovala pred kritickou bezpečnostnou zraniteľnosťou v routroch DSR-150, DSR-150N, DSR-250, DSR-250N a DSR-1000N s ukončenou technickou podporou. Bližšie nešpecifikovaná kritická zraniteľnosť umožňuje vzdialené vykonanie kódu.

Zraniteľnosti v linuxovom nástroji needrestart umožňujú získanie úplnej kontroly nad systémom

Vývojári linuxového nástroja needrestart vydali bezpečnostné aktualizácie, ktoré opravujú 5 zraniteľností. Zraniteľnosti s označením CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, CVE-2024-10224 a CVE-2024-11003 by lokálny autentifikovaný útočník mohol zneužiť na získanie úplnej kontroly nad systémom.

Aktívne zneužívaná zero-day zraniteľnosť v Oracle Agile PLM Framework

Spoločnosť Oracle vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť v produkte Agile Product Lifecycle Management (PLM) Framework. CVE-2024-21287 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom.

.

Kritická zraniteľnosť vo funkcii jazyka PHP

Bezpečnostný výskumník Yiheng Cao objavil kritickú zraniteľnosť vyskytujúcu sa v implementácii PHP funkcie ldap_escape() na 32-bitových systémoch. Táto zraniteľnosť súvisí s pretečením medzipamäte, čo umožňuje zápis do pamäte mimo povolené hodnoty.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v komprimačnom nástroji 7-Zip

Vývojári komprimačného nástroja 7-Zip vydali bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť. CVE-2024-11477 možno podvrhnutím špeciálne vytvorených súborov zneužiť na vzdialené vykonanie kódu.

Kritické zraniteľnosti bezdrôtových prístupových bodov Advantech EKI

Spoločnosť Advantech vydala bezpečnostné aktualizácie na svoje priemyselné bezdrôtové prístupové body (access pointy) série EKI, ktoré opravujú 20 zraniteľností, z čoho 6 je označených ako kritické. CVE-2024-50370 až CVE-2024-50375 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Aktívne zneužívaná zraniteľnosť v platforme ProjectSend

Bezpečnostní výskumníci zo spoločnosti VulnCheck varovali pred aktívnym zneužívaním kritickej zraniteľnosti v open source platforme pre zdieľanie súborov ProjectSend. CVE-2024-11680 možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

Kritické zraniteľnosti v produktoch QNAP

Spoločnosť QNAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 8 zraniteľností, z čoho 3 sú označené ako kritické. Kritické zraniteľnosti v produkte Notes Station 3 (CVE-2024-38643, CVE-2024-38645) a routeroch QuRouter (CVE-2024-48860) možno zneužiť na realizáciu SSRF útokov, získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti vo WordPress plugine Spam Protection, Anti-Spam, FireWall

Vývojári WordPress pluginu Spam Protection, Anti-Spam, FireWall vydali bezpečnostné aktualizácie, ktoré opravujú 2 kritické zraniteľnosti. Zraniteľnosti s označením CVE-2024-10542 a CVE-2024-10781 možno zneužiť na inštaláciu, odstránenie, aktiváciu a deaktiváciu ľubovoľných pluginov redakčného systému a následné získanie úplnej kontroly nad systémom.

Kritické zraniteľnosti v monitorovacej platforme Zabbix

Vývojári monitorovacej platformy Zabbix vydali bezpečnostné aktualizácie, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako kritické. Kritické zraniteľnosti s identifikátormi CVE-2024-42330 a CVE-2024-42327 možno zneužiť na eskaláciu privilégií, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

MESAČNÍK ZRANITEĽNOSTÍ NOVEMBER 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
   - QNAP QuRouter
   - prístupové body Cisco Catalyst IW9165D, Catalyst IW9165E a Catalyst IW9167E s Cisco Unified Industrial Wireless Software
   - SQLite
   - prístupové body Aruba Series 103, 110, 120, 130, 200, 207, 210, 220, 300, 303, 310, 320, 330, 340, 500, 510, 530, 550, 630 a 650 s operačným systémom Instant AOS-8 a AOS-10
   - Veeam Backup Enterprise Manager
   - Ivanti Endpoint Manager, Ivanti Connect Secure, Ivanti Policy, Ivanti Secure Access Client
   - D-Link DSL6740C
   - Adobe Bridge, Adobe Audition, Adobe After Effects, Adobe Substance 3D Painter, Adobe Illustrator, Adobe InDesign, Adobe Commerce, Magento Open Source, Adobe Photoshop
   - .NET, Azure CycleCloud, Azure Database for PostgreSQL Flexible Server, Azure Linux, CBL Mariner, LightGBM, Microsoft 365 Apps for Enterprise, Microsoft Defender for Endpoint, Microsoft Excel, Microsoft Exchange Server, Microsoft Office, Microsoft Office LTSC, Microsoft Office Online Server, Microsoft PC Manager, Microsoft SQL Server, Microsoft SharePoint, Microsoft TorchGeo, Microsoft Visual Studio, Microsoft Word, Python extension for Visual Studio Code, Visual Studio Code, Windows, Windows Server, airlift.microsoft.com
   - Palo Alto Networks PAN-OS
   - PostgreSQL
   - WordPress plugin Really Simple Security
   - GV-VS12, GV-VS11, GV-DSP_LPR_V3, GVLX 4 V2, GVLX 4 V3
   - querydsl-jpa, querydsl-apt, hibernate-core, jakarta.persistence-api, postgresql, OpenFeign querydsl
   - iOS, iPadOS, macOS, visionOS, Safari

- D-Link DSR-150, D-Link DSR-150N, D-Link DSR-250, D-Link DSR-250N, D-Link DSR-500N, D-Link DSR-1000N
- needrestart
- Oracle Agile PLM Framework
- PHP
- 7-Zip
- prístupové body EKI-6333AC-2G, EKI-6333AC-2GD, EKI-6333AC-1GPO
- ProjectSend vo verziách starších ako r1720
- QNAP Notes Station 3, QuRouter, QNAP AI Core, QuLog Center
- WordPress plugin Spam Protection, Anti-Spam, FireWall
- Zabbix

https://csirt.sk/posts/1792.html