CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JÚL 2024

TLP: WHITE

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

1 Globálny výpadok ako následok aktualizácie EDR riešenia

Aktualizácia bezpečnostného nástroja CrowdStrike Falcon nasadeného na operačných systémoch Windows spôsobila masívne výpadky systémov a služieb po celom svete.

2 EUROPOL deaktivoval približne 600 Cobalt Strike serverov

EUROPOL s partnermi v rámci akcie „Operation Morpheus“ zakročili proti prevádzkovateľom nelegálnych Cobalt Strike serverov.

3 Výskumníci zabránili supply chain útoku na Python

Bezpečnostní výskumníci odhalili autentifikačný token pre službu Github, ktorý umožňoval získanie administrátorského prístupu ku kľúčovým repozitárom programovacieho jazyka Python.

4 Pokročilý phishing využíva škodlivé aplikácie aj AI

Kyberkriminálna skupina GXC TEAM poskytuje malware-as-a-service služby kombinujúce phishingové frameworky so škodlivými Android aplikáciami a umelou inteligenciou.

5 Spoločnosť Sekoia spustila riadené odstraňovanie malvéru PlugX

Francúzska polícia, EUROPOL a spoločnosť SEKOIA spustili proces riadeného odstraňovania malvéru PlugX, do ktorého sa zapojili viaceré štáty EÚ.

6 Severokórejský špión sa pokúsil infiltrovať americkú spoločnosť

Americká spoločnosť KNOWBE4 informovala, že osoba, ktorú nedávno prijali na pracovnú pozíciu softvérového inžiniera na prácu z domu, bola v skutočnosti severokórejský špión.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci júl 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. Prihlasovacie údaje k časti takýchto účtov sa vyskytli v predajných ponukách na hackerských fórach.

Stálicou je phishingová kampaň zameraná na občanov Slovenskej republiky, v ktorej útočníci, predstierajúci totožnosť Europolu a vysokopostavených členov Polície SR, posielajú svojim obetiam falošné predvolania kvôli prechovávaniu detskej pornografie a podobným sexuálnym deliktom.

Kurióznym prípadom bolo zahltenie mailového konta zamestnanca organizácie v konštituencii VJ CSIRT vyše 100 000 kópiami rovnakého podvodného e-mailu. Vyšetrovanie prípadu ukázalo, že sa jednalo o konfiguračnú chybu antimalvérového riešenia a nešlo o aktivitu útočníka.

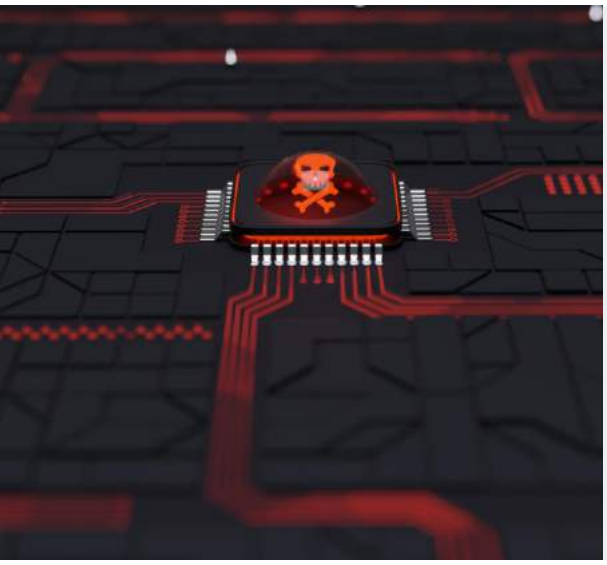
V júli sa objavil tiež útok typu DDoS, ktorý na krátky čas znefunkčnil webovú stránku Ministerstva vnútra SR. K útoku sa neprihlásila žiadna zo známych hacktivistických skupín.

Častým fenoménom vo svete kybernetickej bezpečnosti sú úniky databáz webových služieb a portálov. V tejto súvislosti, na základe našich pozorovaní, chceme upozorniť používateľov, aby nepoužívali svoje pracovné e-mailové adresy (a už vôbec nie rovnaké heslá ako ku pracovným účtom) pre registráciu na webových portáloch pre súkromné účely.

Júl poznamenal aj rozsiahly brute-force útok na e-mailové kontá zamestnancov štátnej organizácie, ktorý pochádzal najmä z dvoch IP adries zo slovenského rozsahu. V takýchto prípadoch VJ CSIRT poskytuje svoje analýzy Policajnému zboru SR.

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



EUROPOL deaktivoval približne 600 Cobalt Strike serverov

EUROPOL a medzinárodné konzorcium pozostávajúce z orgánov činných v trestnom konaní a popredných spoločností pôsobiacich v oblasti kybernetickej bezpečnosti v rámci akcie OPERATION MORPHEUS zakročili proti prevádzkovateľom nelegálnych COBALT STRIKE serverov. Na základe tlačovej správy bolo identifikovaných 690 serverov v 27 štátoch, z ktorých sa koncom júna 2024 podarilo úspešne deaktivovať približne 600. Uvedené servery kyberkriminálnici zneužívali na šírenie rôznych foriem malvéru, vrátane nebezpečných ransomvérov RYUK a CONTI.

Údaje z malvéru ako nástroj pre identifikáciu páchateľov trestnej činnosti

Bezpečnostní výskumníci zo spoločnosti RECORDED FUTURE na základe analýzy dát exfiltrovaných rôznymi rodinami malvéru za obdobie medzi februárom 2021 a 2024 identifikovali viacero páchateľov trestnej činnosti súvisiacej so šírením detskej pornografie. Následnou OSINT analýzou sa ich podarilo bližšie stotožniť a všetky zistenia boli poskytnuté orgánom činným v trestnom konaní. Monitoring exfiltrovaných dát predstavuje veľmi cenný zdroj informácií, ktorý spracovávajú všetky popredné threat intelligence platformy. Uvedeným postupom možno identifikovať nielen obete, ale aj útočníka či páchateľov inej trestnej činnosti. Z právneho hľadiska sa však jedná o „šedú zónu“, nakoľko pri analýze dochádza k prihlasovaniu sa do systémov útočníka.

Austrália varuje pred útokmi čínskej APT40

Medzinárodné konzorcium OČTK vydalo varovanie pred aktivitami čínskej štátom sponzorovanej skupiny APT40, ktorá kompromituje SOHO routre a tie následne zneužíva na realizáciu ďalších útokov a kyberšpionáž. Skupina dlhodobo na prienik do systémov zneužíva zraniteľnosti verejne dostupných služieb a zariadení. Po úspešnom prieniku nasadzuje webshelly, prostredníctvom tzv. kerberoastingu získava prihlasovacie údaje a v rámci laterálneho pohybu po sieti využíva protokol RDP. Vysokú sofistikovanosť útočníka potvrdzuje aj skutočnosť, že po dokončení exfiltrácie dát digitálne stopy zahladzuje vymazávaním logov. Varovanie obsahuje popis techník, taktík a postupov útočníka (TTP) a preventívne odporúčania na zabezpečenie systémov.

VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť Apple nepriamo podporila cenzúru obsahu v Rusku

Spoločnosť APPLE v rámci kybernetického priestoru Ruskej federácie odstránila zo svojho obchodu mobilných aplikácií 25 VPN aplikácií, ktoré agentúra ROSKOMNADZOR označila za nástroje umožňujúce prístup k nelegálnemu obsahu. Vývojári viacerých VPN riešení sa voči tomuto kroku verejne ohradili a upozornili, že spoločnosť Apple je v záujme udržania si ruského trhu ochotná vyhovieť aj sporným požiadavkám ruskej vlády, ktoré obmedzujú voľný prístup k informáciám a podporujú cenzúru obsahu.

Celosvetový výpadok služieb ako následok aktualizácie CrowdStrike Falcon

Aktualizácia bezpečnostného nástroja CrowdStrike Falcon nasadeného na operačných systémoch Windows spôsobila masívne výpadky systémov a služieb po celom svete. Výpadky nastali 19. júla 2024 po publikovaní aktualizácie. Chyba sa podľa spoločnosti nachádzala v ovládači C-00000291*.sys a spôsobila, že zasiahnuté systémy zostali v slučke bootovania a zobrazovali chybové hlásenie. Vzhľadom na potenciálne zneužitie vzniknutej situácie na realizáciu kybernetických útokov, vládna jednotka CSIRT na svojej webovej stránke zverejnila varovanie, ktoré obsahovalo aj návod na mitigáciu problému. Útočníci výpadok využili aj v rámci phishingových kampaní.

Malvér SYS01 cieli špecificky na používateľov sociálnej siete Facebook

Spoločnosti TRUSTWAVE SPIDERLABS zverejnila analýzu phishingovej kampane, v rámci ktorej útočníci zneužívajú kompromitované účty a reklamný obsah platformy Facebook na šírenie malvéru SYS01. Kampaň sa tematicky zameriava na obete vyhľadávajúce grafické témy operačného systému Windows alebo pirátske kópie licencovaných softvérov. Analyzovaný variant SYS01 bol špeciálne navrhnutý na získanie kontroly nad Facebook účtami, krádež prihlasovacích údajov z prehliadača a ich následné zneužitie na ďalšie šírenie. Nárast početnosti kampaní, ktoré na šírenie phishingového a škodlivého obsahu využívajú reklamné platformy spoločností META a GOOGLE z dlhodobého hľadiska pozoruje aj Vládna jednotka CSIRT.

VÝZNAMNÉ UDALOSTI VO SVETE

Útočník zneužíva nezabezpečené API rozhrania na získavanie citlivých údajov

Útočník, ktorý na hackerskom fóre BREACHFORUMS vystupuje pod aliasom EMO, sa zameriava na vyhľadávanie a zneužívanie nezabezpečených API rozhraní. Týmto postupom exfiltroval a zverejnil citlivé údaje používateľov služieb Trello od spoločnosti Atlassian (zasiahnutých 15 miliónov používateľov) a Life360 (zasiahnutých 500 tisíc používateľov). Zverejnená množina dát obsahovala mená, e-mailové adresy, telefónne čísla a ďalšie metadáta, ktoré je možné zneužiť na prípravu cielených phishingových kampaní. Vládna jednotka CSIRT vykonala analýzu zverejnených údajov, identifikovala a notifikovala obete z kybernetického priestoru SR.

Výskumníci zabránili supply chain útoku na používateľov jazyka Python

Bezpečnostní výskumníci zo spoločnosti JFROG LTD v rámci vyhľadávania prístupových údajov vo verejne dostupných zdrojoch odhalili autentifikačný token pre službu Github, ktorý umožňoval získanie administrátorského prístupu ku kľúčovým repozitárom programovacieho jazyka PYTHON (PYPA, PSF a PYPI). Vývojári Python na upozornenie pohotovo zareagovali a podarilo sa tak zabrániť potenciálnemu supply chain útoku veľkých rozmerov. Uvedený incident zdôrazňuje význam dodržiavania pravidiel bezpečného programovania a možnosti praktického využitia analýzy zdrojového kódu programov, knižníc, obrazov kontajnerizačných riešení a binárnych súborov, ktorú vykonávajú aj útočníci.

Zraniteľnosť aplikácie Telegram umožňovala maskovanie APK súborov za videá

Spoločnosť ESET zverejnila informácie o zero-day bezpečnostnej zraniteľnosti aplikácie TELEGRAM s označením EvilVideo, ktorá umožňovala maskovanie APK súborov za videá vo formáte MP4. Zraniteľné boli len verzie aplikácie pre operačné systémy ANDROID. Proof-of-Concept kód demonštrujúci návod na jej zneužitie bol od 6. júna 2024 na predaj na ruskom hackerskom portály XSS. Vývojári Telegram vydali bezpečnostné aktualizácie až 11. júla 2024, čo útočníkom dávalo približne 5 týždňov na jej zneužitie v rámci útokov. Zneužitie zraniteľnosti vyžadovalo interakciu zo strany používateľa, ktorý musel potvrdiť sériu upozornení.

VÝZNAMNÉ UDALOSTI VO SVETE

Phishingová kampaň zneužívajúca chaos spôsobený updatom CrowdStrike Falcon

Spoločnosť CROWDSTRIKE varovala pred masívnou phishingovou kampaňou s tématikou obnovy zariadení zasiahnutých výpadkom, ktorej cieľom bola inštalácia malvéru DAOLPU. Phishingové e-maily obsahovali škodlivú .DOCM prílohu, teda WORD súbor obsahujúci makrá. Samotný dokument okrem kópie oficiálneho návodu od spoločnosti MICROSOFT obsahoval aj makrá na stiahnutie DLL knižnice zakódovanej prostredníctvom BASE64. CrowdStrike túto informáciu zverejnila po identifikácii chyby validačného mechanizmu pre aktualizačné súbory senzora, ktorý spôsobil globálny výpadok na zariadeniach s OS Windows.

Kryptoburzy čelia phishingovej kampani zneužívajúcej falošné DNS záznamy

Kryptoburza DYDX varovala svojich používateľov, že útočníci kompromitovali webovú stránku staršej verzie ich platformy s označením v3. Podľa zverejnených informácií útočníci získali kontrolu nad DNS záznamami, ktoré zneužili na presmerovanie používateľov na phishingovú stránku slúžiacu na získavanie prístupových údajov. Incident súvisí s nedávnou vlnou rovnakých útokov využívajúcich falošné DNS záznamy (tzv. DNS hijacking) cielených aj na ďalšie kryptoburzy, pričom všetky zasiahnuté domény sú v súčasnosti v správe doménového registrátora SQUARESPACE. Na základe dostupných informácií boli ohrozené všetky domény, ktoré boli po minuloročnej dohode so spoločnosťou Google zmigrované na Squarespace. Doménový administrátori by mali na svojich kontách aktivovať mechanizmy viacfaktorovej autentifikácie.

Nový zamestnanec spoločnosti KNOWBE4 bol v skutočnosti severokórejským špiónom

Americká spoločnosť KNOWBE4 informovala, že osoba, ktorú nedávno prijali na pracovnú pozíciu softvérového inžiniera na prácu z domu, bola v skutočnosti severokórejskou vládou podporovaný útočník. V rámci pohovoru prešiel viacerými kolami, pričom využil údaje generované prostredníctvom umelej inteligencie. Útočník sa po doručení služobného počítača pokúsil o infikovanie zariadení spoločnosti bližšie nešpecifikovaným malvérom slúžiacim na exfiltráciu dát uložených vo webovom prehliadači. Aktivity útočníka však boli zachytené v rámci SOC monitoringu, čo zabránilo rozsiahlejšej kompromitácii. Na podobné špionážne aktivity americká FBI opakovane upozorňuje už od roku 2023.

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

VÝZNAMNÉ UDALOSTI VO SVETE

USA pridalo kľúčových členov ruskej hacktivistickej skupiny na sankčný zoznam

Americká vláda pridala dvoch kľúčových členov prorusky orientovanej hacktivistickej skupiny CYBER ARMY OF RUSSIA REBORN na zoznam sankcií. Prvou osobou je YULIYA PANKRATOVA vystupujúca pod aliasom „YuliYA“, ktorá je považovaná za vodkyňu a hovorkyňu skupiny. Druhou osobou je DENIS DEGTYARENKO vystupujúci pod aliasom „Dena“, ktorý je považovaný za hlavného hackera a tvorcu vzdelávacích materiálov. Skupina začala v roku 2022 realizáciou DDoS útokov a postupne sa dopracovala až k útokom na prvky kritickej infraštruktúry. Medzi historické, aj potenciálne budúce ciele DDoS útokov tejto skupiny patrí aj Slovenská republika.

Slovenská republika zapojená do riadeného odstraňovania malvéru PlugX

Francúzska polícia, EUROPOL a spoločnosť SEKOIA spustili proces riadeného odstraňovania malvéru PLUGX. Sekoia v apríli 2024 získala kontrolu nad jedným z riadiacich serverov tohto malvéru, čo jej umožnilo monitorovať sieťovú komunikáciu a identifikovať infikované zariadenia po celom svete. Informácie o obetiach zdieľala s orgánmi činnými v trestnom konaní a navrhla proces riadenej dezinfekcie založený na využití zabudovanej funkcionality riadiaceho panelu. Do procesu odstraňovania sa zapojili viaceré štáty EÚ - Francúzsko, Malta, Portugalsko, Chorvátsko, Rakúsko, vrátane Slovenskej republiky.

Skupina GXC predáva pokročilé phishingové frameworky so škodlivými Android aplikáciami

Kyberkriminálna skupina GXC TEAM poskytuje malware-as-a-service služby kombinujúce phishingové frameworky so škodlivými ANDROID aplikáciami. Pokročilé funkcie frameworku útočníkom umožňujú monitorovať priebeh kampane v reálnom čase a využitím umelej inteligencie realizovať dôveryhodne znejúce telefonické volania. Jedným z krokov je aj inštalácia mobilného malvéru, ktorý po inštalácii pýta povolenie byť predvolenou aplikáciou pre prácu so SMS, čo umožňuje zachytávanie a exfiltráciu citlivých údajov, vrátane OTP kódov pre rôzne služby. Jedná o dynamicky sa rozvíjajúcu skupinu, ktorá predáva aj phishingový framework zneužívajúci identitu slovenskej banky ČSOB.

VÝZNAMNÉ UDALOSTI VO SVETE

X bez povolenia trénuje AI model GROK na základe príspevkov používateľov X

Spoločnosť X začala trénovať svoj AI model GROK na verejných príspevkoch platformy X bez explicitného informovania svojich používateľov. Trénovanie odhalili používatelia, ktorí v nastaveniach našli prepínač povoľujúci využitie príspevkov pre trénovanie AI, ktorý bol dokonca predvolene zapnutý. Spoločnosť X zareagovala vyhlásením, že používatelia majú možnosť vyňať svoje príspevky z trénovania a prepínač bude čoskoro dostupný aj na mobilných klientoch. Znepokojujúce je, že nakoľko je prepínač predvolene zapnutý, spoločnosť X mohla uvedeným spôsobom už trénovať svoj model dlhšiu dobu. Írske orgány na ochranu osobných údajov začali vyšetrovanie a v závislosti od zistení spoločnosti X hrozia aj finačné pokuty.

Chyba v Github umožňuje obnovu obsahu z vymazaných repozitárov a forkov

Bezpečnostní výskumníci odhalili nedostatok platformy GITHUB, ktorý možno zneužiť na získanie obsahu z vymazaných repozitárov a z forkov. V súvislosti so svojimi zisteniami navrhli zavedenie nového CWE označenia CFOR (Cross Fork Object Reference), ktorý označuje zraniteľnosť umožňujúcu prístup k citlivým údajom z iného forku, vrátane privátnych a vymazaných forkov. Spoločnosť MICROSOFT sa vyjadrila, že sa jedná o očakávané správanie platformy a súvisí s princípom fungovania GIT, konkrétne s tzv. dangling commit. Článok referencuje aj online databázu GHARCHIVE.ORG, ktorá zaznamenáva všetky akcie na platforme GITHUB a je potenciálnym zdrojom dát pre útočníkov aj bezpečnostných výskumníkov.

Proofpoint odstránila problém zneužívaný na rozposielanie phishingových e-mailov

Spoločnosť PROOFPOINT vydala aktualizácie svojich mailových relay serverov (*.pphosted.com), ktoré opravili administratívne rozhranie pre konfiguráciu smerovania e-mailov a nesprávne vyhodnocovanie SPF pravidiel obsahujúcich MICROSOFT 365 tenanty. SPF pravidlá umožňovali preposielanie odchádzajúcich e-mailov zo všetkých MS365 tenantov, čo bližšie nešpecifikovaný útočník od januára 2024 aktívne zneužíval na rozposielanie phishingových e-mailov v rámci kampane označenej ECHOSPOOFING. Nové nastavenia blokujú všetky MS 365 tenanty mimo používateľom definovaného zoznamu. Bezpečnostná komunita následne zistila, že sa problém týka aj viacerých poskytovateľov služieb a zraniteľnostiam boli priradené identifikátory CVE-2024-7208 a CVE-2024-7209.

VÝZNAMNÉ UDALOSTI VO SVETE

- Nezabezpečené API rozhranie umožnilo identifikáciu 33 miliónov používateľov viacfaktorovej autentifikačnej služby Authy od spoločnosti Twilio
- Vývojári Signal implementovali dodatočné zabezpečenie databázy správ na desktopových verziách svojej aplikácie (Signal Desktop pre Windows a Mac)
- Spoločnosť Avast zverejnila dekryptor pre ransomvér DONEX, ktorý bol vytvorený na základe chyby kryptografickej schémy používanej v rámci šifrovania súborov
- Bezpečnostní výskumníci zverejnili analýzu malvéru FROSTYGOOP, ktorý útočníci v januári 2024 zneužili na vyradenie systémov kúrenia v meste Ľvov
- Spoločnosť Eset varovala pred tzv. malwaretisement kampaňami cielenými na používateľov populárnej mobilnej aplikácie HAMSTER KOMBAT
- Bezpečnostní výskumníci informovali o tzv. card skimming kampani cielenej na webové stránky na báze redakčného systému Magenta
- Hackerská skupina STARGAZER GOBLIN prevádzkuje sieť pre šírenie malvéru, ktorá je založená na falošných Github repozitároch a kompromitovaných Wordpress stránkach
- Útočníci aktívne zneužívajú zraniteľnosť CVE-2024-21412 v produkte Microsoft Defender Smartscreen na šírenie malvérov ACR STEALER, LUMMA a MEDUZA
- Bezpečnostní výskumníci upozornili na bezpečnostné riziko aplikácie WhatsApp for Windows, ktoré umožňuje priame spustenie PYTHON a PHP skriptov
- Spoločnosť DigiCert bude z dôvodu chyby súvisiacej s overovaním vlastníctva domén cez CNAME záznamy revokovať SSL/TLS certifikáty viacerých subjektov

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v Docker Engine

Vývojári kontajnerizačnej technológie Docker Engine vydali bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť. CVE-2024-41110 možno zneužiť na obídenie autorizačných pluginov AuthZ a eskaláciu privilégií. Jedná sa o opätovný výskyt zraniteľnosti odstránenej v januári 2019, ktorej oprava nebola zakomponovaná do novších verzií Docker Engine 19.03 a vyššie.

Zraniteľnosti v serveroch Atlassian

Spoločnosť Atlassian vydala bezpečnostné aktualizácie svojich produktov Bamboo Data Center a Server, Confluence Data Center a Server, Jira Data Center and Server a Jira Service Management Data Center a Server, ktoré opravujú 30 zraniteľností. Najzávažnejšie zraniteľnosti nachádzajúce sa v Bamboo Data Center a Server možno zneužiť na realizáciu SSRF útokov, vzdialené vykonanie lokálnych súborov a získanie neoprávneného prístupu do systému.

Kritické zraniteľnosti v produktoch SolarWinds Access Rights Manager

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie produktu SolarWinds Access Rights Manager, ktoré opravujú 13 zraniteľností, z toho 8 označených ako kritické. Kritické zraniteľnosti možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

Kritické zraniteľnosti v produktoch Cisco Security Email Gateway a Cisco Smart Software Manager On-Prem

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú zraniteľnosti v produktoch Cisco Secure Email Gateway a Cisco Smart Software Manager On-Prem. CVE-2024-20401 a CVE-2024-20419 by vzdialený útočník mohol zneužiť na modifikáciu súborov na súborovom systéme zariadení a získanie neoprávneného prístupu do systému.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť servera Exim

Mailový server Exim obsahuje zraniteľnosť, ktorá umožňuje útočníkom doručiť obetiam do mailboxu súbory so zakázanou príponou. Ochranou servera prejdú aj škodlivé spustiteľné súbory.

Kritická bezpečnostná zraniteľnosť v OpenSSH

Vývojári nástroja OpenSSH vydali bezpečnostnú aktualizáciu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť. Zraniteľnosť možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad zraniteľným systémom. Bezpečnostní výskumníci počas jej detailnej analýzy odhalili aj jej menej závažný variant CVE-2024-6387 s označením CVE-2024-6409, ktorý taktiež možno zneužiť na vykonanie kódu.

Citrix opravila viacero zraniteľností svojich produktov

Spoločnosť Citrix opravila kritické a vysoko závažné zraniteľnosti vo viacerých svojich produktoch. Zraniteľnosti umožňujú útočníkom získať privilégiá na úrovni SYSTEM, presmerovať používateľov na škodlivé webstránky, získať citlivé údaje alebo spôsobiť nedostupnosť systému.

Vysoko závažné zraniteľnosti SAP

Spoločnosť SAP vydala v júli 2024 balík opráv pre svoje produkty opravujúcich 16 zraniteľností v aplikáciách PDCE, Commerce, Landscape Management, Document Builder, NetWeaver Knowledge Management XMLEditor a ďalších. 2 z nich sú označené ako vysoko závažné. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi čítať všeobecné údaje z tabuľky alebo pristupovať k nesprávne nakonfigurovaným stránkam. Na zraniteľnosť upozornila spoločnosť Onapsis Research Labs (ORL).

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Microsoft v rámci júlového Patch Tuesday opravil kritické a zero-day zraniteľnosti

Spoločnosť Microsoft vydala v júli 2024 balík opráv pre portfólio svojich produktov opravujúci 139 zraniteľností, z ktorých 54 umožňuje vzdialené vykonávanie kódu. Zero-day zraniteľnosti s označením CVE-2024-38080 a CVE-2024-38112 sú aktívne zneužívané útočníkmi.

Kritická zraniteľnosť protokolu RADIUS

Tím výskumníkov popísal útok na protokol RADIUS, ktorým môže útočník pomocou manipulácie prefixu paketu a vytvorením kolízie MD5 pre premennú v ňom zakomponovanú získať povolenie na prístup do administrátorského rozhrania sieťového zariadenia. Útočník nepotrebuje poznať heslo ani zdieľané tajomstvá.

Aktívne zneužívaná zero-day zraniteľnosť v prepínačoch CISCO NEXUS a MDS

Spoločnosť CISCO vydala bezpečnostné aktualizácie na sieťové prepínače série NEXUS a MDS, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť umožňujúcu vykonanie škodlivého kódu. Bezpečnostní výskumníci zo spoločnosti SYGNIA evidujú prípady jej úspešného zneužitia zo strany čínskej skupiny VELVET ANT.

MESAČNÍK ZRANITEĽNOSTÍ JÚL 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
   - Docker Engine, Docker Desktop
   - Bamboo Data Center a Server, Confluence Data Center a Server, Jira Data Center a Server, Jira Service Management Center a Server
   - SolarWinds Access Rights Manager
   - Cisco Secure Email Gateway, Cisco Smart Software Manager On-Prem
   - Server Exim
   - OpenSSH
   - NetScaler ADC, NetScaler Gateway, NetScaler Console, NetScaler SVM, NetScaler Agent, Citrix Workspace, Citrix Provisioning, Citrix Virtual Apps and Desktops, Citrix Workspace pre Windows
   - SAP PDCE, SAP Commerce, SAP Landscape Management, SAP Document Builder, SAP NetWeaver Knowledge Management XMLEditor, SAP CRM WebClient UI, SAP Business Warehouse – Business Planning and Simulation, SAP S/4HANA Finance, SAP Business Workflow, SAP GUI for Windows, SAP Transportation Management, SAP Enable Now
   - .NET 8.0, Azure CycleCloud, Azure DevOps Server, Azure Kinect SDK, Azure Network Watcher VM Extension for Windows, Microsoft .NET Framework, Microsoft 365, Microsoft Defender for IoT, Microsoft Dynamics 365 (on-premises), Microsoft OLE DB Driver, Microsoft Office, Microsoft Outlook, Microsoft SQL Server, Microsoft SharePoint Enterprise Server, Microsoft SharePoint Server, Microsoft Visual Studio, Windows, Windows Server
   - RADIUS protokol
   - CISCO Nexus, CISCO MDS 9000

https://www.csirt.gov.sk/posts/1203.html