CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

JÚL 2026

TLP: CLEAR

Kybernetickým priestorom v júli 2026 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Zero-click zraniteľnosť v Zimbre zneužívajú ruskí útočníci na krádež e-mailov

Ruská štátom podporovaná skupina Laundry Bear (Void Blizzard) aktívne zneužíva zero-click zraniteľnosť CVE-2025-66376 v aplikácii Zimbra Collaboration na krádež e-mailov, prihlasovacích údajov a obnovovacích kódov dvojfaktorovej autentifikácie.

2 Ruská skupina Gamaredon rozšírila špionážne kapane proti ukrajinským vládnym a vojenským organizáciám

Ruská APT skupina Gamaredon počas roka 2025 výrazne rozšírila svoje kyberšpionážne operácie proti Ukrajine, pričom výskumníci zaznamenali 35 spear-phishingových kampaní zameraných najmä na vládne a vojenské organizácie.

3 Ruská spravodajská služba sleduje logistické trasy cez IP kamery v krajinách NATO a na Ukrajine

Ruská spravodajská služba systematicky kompromituje internetom pripojené IP kamery v krajinách NATO a na Ukrajine, aby sledovala vojenské logistické trasy, presuny zbraní a polohu ukrajinských jednotiek.

4 Americké bezpečnostné služby upozorňujú na phishingové kampane ruských spravodajských skupín v aplikácii Signal

FBI a CISA upozorňujú, že ruské spravodajské skupiny sa v aplikácii Signal snažia vylákať obnovovacie kľúče záloh a prevziať tak kontrolu nad účtami vládnych predstaviteľov, vojakov, politikov a novinárov.

5 Falošná IT podpora cez Microsoft Teams šíri malvér Etherrat

Útočníci sa cez hlasové hovory v Microsoft Teams vydávajú za pracovníkov IT podpory a presviedčajú zamestnancov, aby si nainštalovali malvér EtherRAT, čím získajú počiatočný prístup do firemných sietí.

6 Microsoft ukončí bezpečnostné aktualizácie pre exchange 2016 a 2019 v októbri 2026

Program Extended Security Updates pre Exchange Server 2016 a 2019 definitívne skončí v októbri 2026, po čom Microsoft prestane vydávať bezpečnostné aktualizácie a organizáciám odporúča prejsť na Exchange Server SE alebo Exchange Online.

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. Jednotka riešila aj prípad spoofovanej e-mailovej adresy IT oddelenia organizácie v konštituencii VJ CSIRT.

Aj tento mesiac sa v rámci zachytených phishingových kampaní vyskytlo viacero pravdepodobne kompromitovaných e-mailových adries, ktoré šírili malvér z rodiny Agent Tesla. Jedná sa o trójsky kôň pre vytvorenie vzdialeného prístupu ku infikovanému zariadeniu. Tento malvér bol prvýkrát pozorovaný v roku 2014. Časť e-mailových správ bola zachytená v karanténe. Podľa dostupných logov však niektoré správy detekciu a karanténu obišli. Z poskytnutých vzoriek správ boli extrahované indikátory kompromitácie, ktoré boli publikované prostredníctvom platformy Afrodita MISP.

Jednotka CSIRT.SK prijala hlásenie organizácie vo svojej konštituencii o kampani podvodných e-mailov, ktoré smerovali na kontá jej zamestnancov. E-maily imitovali výpisy z účtu Slovenskej sporiteľne a Tatra Banky. Organizácia vykonala potrebné opatrenia pre mitigovanie hrozby a poskytla vzorku e-mailovej správy na analýzu. Tá ukázala, že príloha e-mailov spúšťala škodlivý kód. Organizácia dostala odporúčania na konkrétne kroky na zamedzenie kompromitácie zariadení, ktorých používatelia prílohu otvorili.

V júli prijala jednotka CSIRT.SK hlásenie o kompromitácii webovej stránky subjektu v jej konštituencii. Organizácia už v júni zaznamenala neštandardné aktivity na danej stránke. Poskytla záznamy z logov a požiadala o súčinnosť pri riešení incidentu. Jednotka poskytla plnú súčinnosť, vykonala analýzu incidentu a poskytla odporúčania pre zamedzenie ďalšej kompromitácie systémov. Jedným z odporúčaní bolo tiež kontaktovať Úrad pre ochranu osobných údajov SR vzhľadom na možný únik údajov. Web bol obnovený zo záloh s kompletnou kontrolou dát a kompletne obnovenou databázou.

Kompromitovaný web hlásila aj ďalšia organizácia. Server, na ktorom sa nachádzala stará a zraniteľná verzia redakčného systému Joomla, uzamkli a vypli jeho sieťové rozhranie. Organizácia naplánovala jeho obnovu zo zálohy s aplikovaním všetkých dostupných bezpečnostných záplat. Jednotka poskytla rad odporúčaní pre riešenie incidentu a obnovu systému. Na kompromitovanej verzii webového servera a aktuálnej Joomla DB vykonala forenznú analýzu.

Do tretice, jednotka prijala od partnera hlásenie o kompromitácii webovej stránky v správe obce. Predmetný web útočníci zneužívali na účely SEO poisoningu. CSIRT.SK vykonala analýzu systému a identifikovala použitý škodlivý obsah, ktorý bežal priamo na webserveri. Útočník vďaka nemu dokázal meniť webový prenos tak, aby vyhľadávačom zobrazil iný obsah než bežným návštevníkom.

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 webových domén, ktorý realizuje modul Domino, a informovanie o únikoch prihlasovacích údajov zozbieraných viacerými službami s celosvetovou pôsobnosťou (Have I Been Pwned, DeHashed, Recorded Future a SocRadar).

.

O službe Achilles napísali pozitívne aj novinári z portálu Živé.sk vo svojom článku v časti Nájsť slabiny pomáha bezplatný systém.

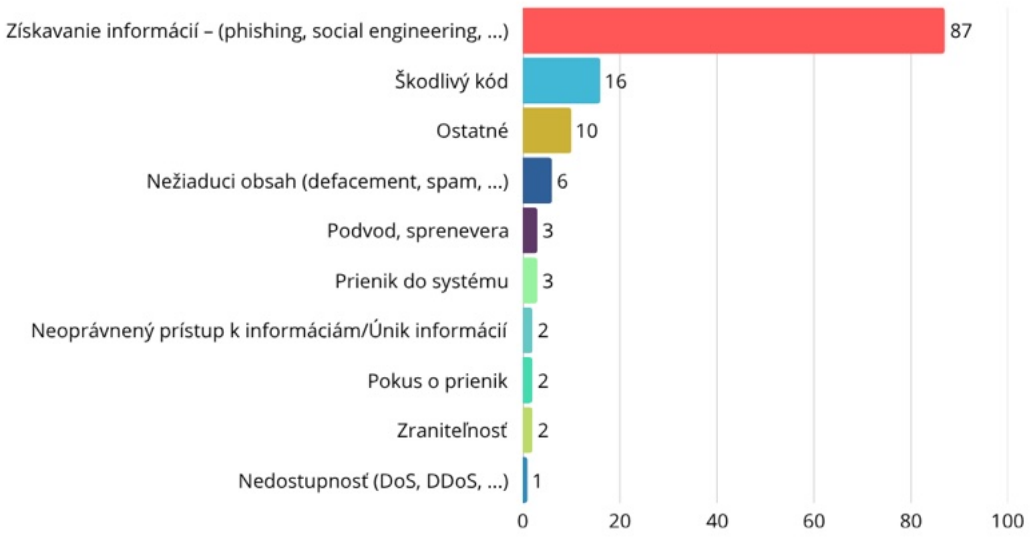
V rámci služby Ares prebiehalo 9 penetračných testov webových aplikácií a infraštruktúry. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

V júli CSIRT.SK plošne varoval svoju konštituenciu ohľadom zraniteľností CVE-2026-63030 a CVE-2026-60137 jadra populárneho redakčného systému WordPress, ktoré dostali názov wp2shell. O chybách zabezpečenia informoval aj na svojej webstránke. Ich zreťazením môže neautentifikovaný útočník získať schopnosť vzdialene vykonávať kód. Pre zraniteľnosti existuje verejne dostupný exploit.

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 júli jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti učiteľom Hotelovej akadémie Mikovíniho 1 v Bratislave.

Členovia tímu CSIRT.SK mali v júli prednášky na konferencii OSSConf, ktorú organizovala Žilinská univerzita. Predstavili v nich služby CSIRT.SK, rozobrali bezpečnostné výzvy využívania AI pri vývoji kódu a ukázali, ako môže vyzerať hackerský útok na wifi a na zraniteľný server.

VJ CSIRT poskytuje tiež školenia a cvičenia pre svoju konštituenciu v rámci výcvikového a školiaceho strediska Kyberaréna.



VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci využívajú manipuláciu výsledkov vyhľadávania

Kampaň zameraná na SEO poisoning manipuluje výsledky vyhľadávania tak, aby používatelia sťahovali infikovaný softvér z falošných alebo kompromitovaných stránok. Útočníci vytvárajú alebo optimalizujú stránky, ktoré sa zobrazujú na popredných miestach vo vyhľadávačoch pre populárne softvérové nástroje. Následne distribuujú trojanizované inštalátory obsahujúce malvér AsyncRAT. Cieľom je masová distribúcia škodlivého kódu cez dôveryhodne pôsobiace sťahovacie portály.

Ruská skupina Gamaredon rozšírila špionážne kampane proti ukrajinským vládnym a vojenským organizáciám

Ruská APT skupina Gamaredon počas roka 2025 výrazne rozšírila svoje kyberšpionážne operácie proti Ukrajine. Výskumníci zo spoločnosti ESET zaznamenali 35 spear-phishingových kampaní zameraných najmä na ukrajinské vládne a vojenské organizácie. Útočníci zneužívali techniku HTML smuggling, zraniteľnosť CVE-2025-8088 vo WinRAR a nové nástroje PowerShell na sťahovanie ďalšieho malvéru, udržiavanie perzistencie a exfiltráciu dát. Skupina zároveň vo väčšej miere využíva legitímne služby ako GoFile, Dropbox, Telegram a Cloudflare Workers na ukrývanie svojej infraštruktúry a komunikácie s riadiacimi servermi. Cieľom kampaní zostáva získavanie citlivých informácií na podporu ruských spravodajských aktivít v súvislosti s vojnou na Ukrajine. generované pomocou AI, čím vzniká nový priestor pre phishing a sociálne inžinierstvo.

Americké bezpečnostné služby upozorňujú na phishingové kampane ruských spravodajských skupín v aplikácii Signal

FBI a CISA upozorňujú, že ruské spravodajské skupiny rozšírili phishingovú kampaň proti používateľom aplikácie Signal. Namiesto prihlasovacích kódov a PIN-ov sa teraz snažia získať obnovovacie kľúče, tzv. Backup Recovery Keys, ktoré im umožnia obnoviť zálohu účtu, získať prístup k celej histórii správ a kompletne nad účtom prevziať kontrolu. Útočníci sa vydávajú za technickú podporu aplikácie Signal. Kampaň cielili najmä na vládnych predstaviteľov, vojakov, politikov, novinárov a ďalšie osoby s vysokou spravodajskou hodnotou. FBI odporúča používateľom, aby obnovovacie kľúče nikdy nezdieľali, ignorovali podozrivé správy a v prípade podozrenia okamžite vygenerovali nový obnovovací kľúč v nastaveniach aplikácie.

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

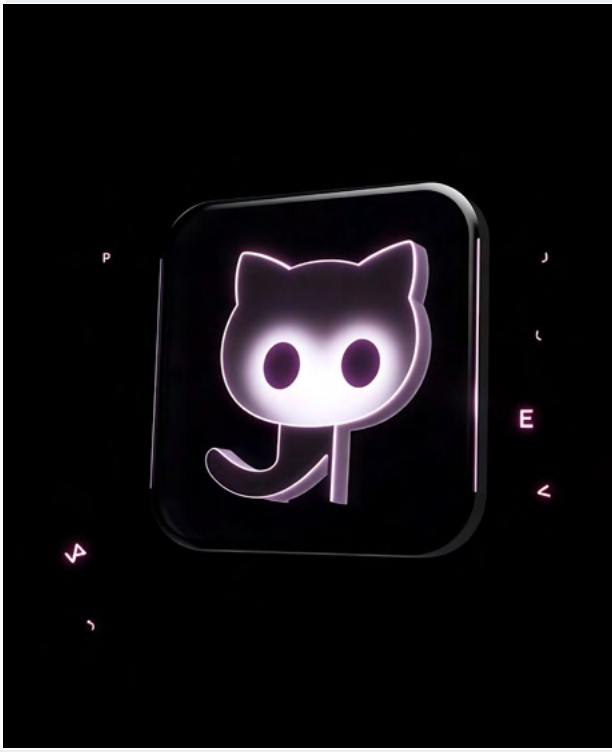
VÝZNAMNÉ UDALOSTI VO SVETE

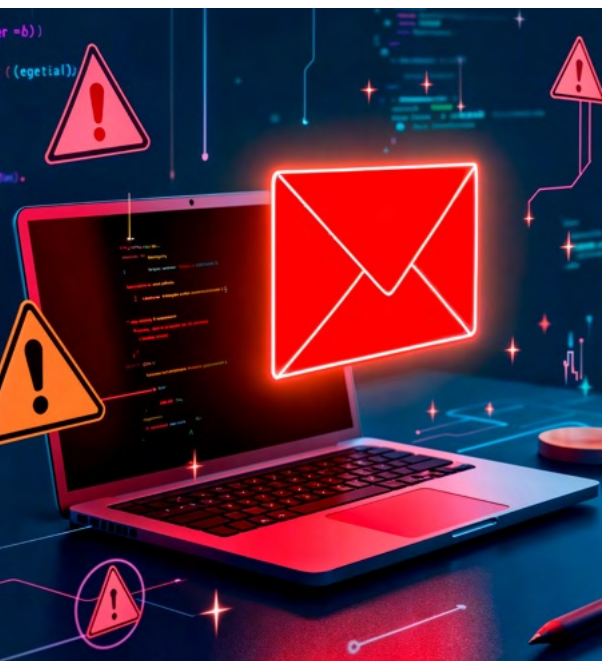
Falošná IT podpora cez Microsoft Teams šíri malvér EtherRAT

Útočníci zneužívajú hlasové hovory v službe Microsoft Teams, pri ktorých sa vydávajú za pracovníkov IT podpory a presviedčajú zamestnancov, aby si nainštalovali malvér EtherRAT, čím získajú počiatočný prístup do firemných sietí. Útok sa začína phishingovým e-mailom s falošným „zamestnaneckým prieskumom", po ktorom nasleduje hovor cez Teams z externého účtu predstierajúceho správcu systému. Útočníci následne využívajú legitímne nástroje na vzdialenú správu a škodlivý Node.js loader na inštaláciu EtherRAT, ktorý umožňuje vzdialené ovládanie zariadenia.

Útočníci zneužívajú stovky falošných GitHub repozitárov na distribúciu malvéru

Bezpečnostní výskumníci odhalili kampaň, v rámci ktorej útočníci vytvorili takmer 300 falošných GitHub repozitárov vydávajúcich sa za legitímne projekty s otvoreným zdrojovým kódom, bezpečnostné nástroje a populárny softvér s cieľom šíriť malvér z kategórie infostealer. Repozitáre obsahovali súbory README, upravenú históriu commitov a odkazy na škodlivé binárne súbory, pričom sa vo výsledkoch vyhľadávania často zobrazovali vedľa originálnych projektov. Po spustení stiahnutých súborov sa do zariadení obetí inštalovali infostealery schopné kradnúť prihlasovacie údaje, kryptomenové peňaženky, uložené heslá a ďalšie citlivé informácie. Výskumníci odporúčajú vývojárom dôkladne overovať dôveryhodnosť repozitárov, kontrolovať vlastníka projektu, históriu vývoja a sťahovať softvér iba z oficiálnych zdrojov, keďže ide o ďalší príklad rastúceho rizika útokov na softvérový dodávateľský reťazec.



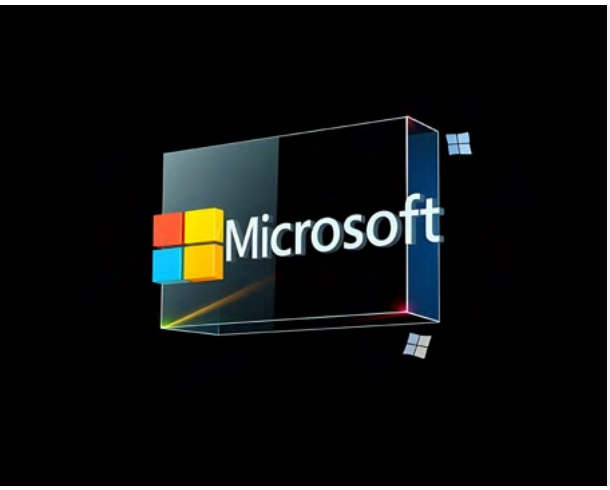


Phishingová kampaň cieli na používateľov LastPass a Bitwarden

Spoločnosť LastPass upozornila na prebiehajúcu phishingovú kampaň, ktorá cieli na používateľov služieb LastPass a Bitwarden prostredníctvom falošných bezpečnostných upozornení. Útočníci rozosielajú e-maily napodobňujúce oficiálnu komunikáciu, informujú o údajných zmenách bezpečnostných pravidiel a vyzývajú adresátov na otvorenie dokumentu cez falošnú stránku imitujúcu DocuSign. LastPass zdôraznil, že jeho systémy nečelili kompromitácii a útočníci iba zneužívajú domény a vizuálne prvky pripomínajúce legitímne firemné služby. Spoločnosť odporúča neotvárať odkazy z nevyžiadaných e-mailov, overovať odosielateľa a prihlasovať sa do účtov výhradne cez oficiálne webové stránky alebo aplikácie.

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

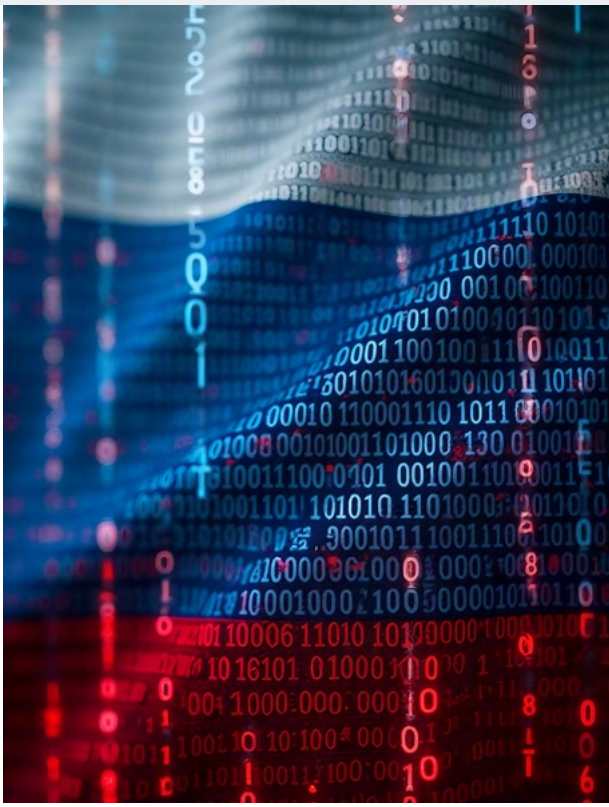
VÝZNAMNÉ UDALOSTI VO SVETE



Microsoft ukončí bezpečnostné aktualizácie pre Exchange 2016 a 2019 v októbri 2026

Microsoft pripomenul, že program Extended Security Updates (ESU) pre Exchange Server 2016 a Exchange Server 2019 definitívne skončí v októbri 2026 a po tomto termíne už nevydá žiadne ďalšie bezpečnostné aktualizácie. Organizáciám preto odporúča prejsť na Exchange Server Subscription Edition (SE) alebo migrovať do Exchange Online v rámci Microsoft 365.

Ruská spravodajská služba sleduje logistické trasy cez IP kamery v krajinách NATO a na Ukrajine

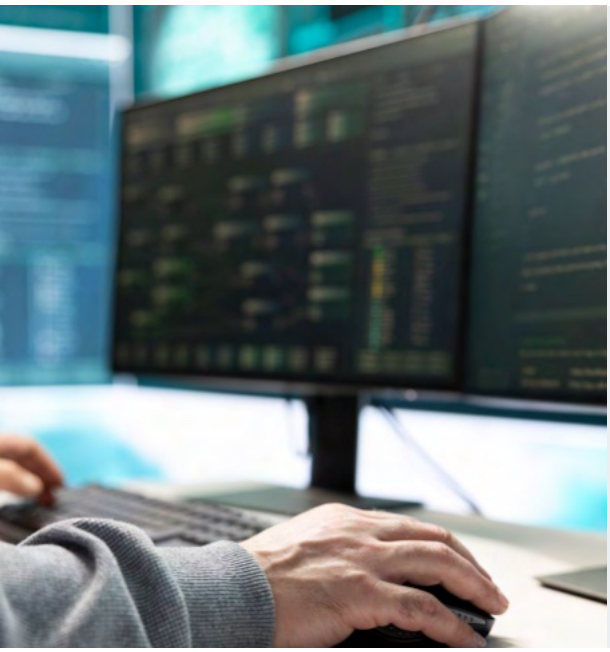


Ruská spravodajská služba systematicky kompromituje IP kamery pripojené na internet v krajinách NATO a na Ukrajine, aby sledovala vojenské logistické trasy, presuny zbraní smerujúcich na Ukrajinu a polohu ukrajinských jednotiek. Vyšetrovanie holandských spravodajských služieb AIVD a MIVD potvrdilo kompromitáciu kamier aj pozdĺž logistických trás v Holandsku. Útočníci získavajú prístup najmä prostredníctvom známych zraniteľností, slabých alebo predvolených hesiel a nesprávne nakonfigurovaných zariadení. Spoločné odporúčanie bezpečnostných orgánov vyzýva organizácie na okamžitú aktualizáciu firmvéru, zmenu predvolených prihlasovacích údajov, vypnutie vzdialeného prístupu z internetu a ochranu zariadení pomocou viacfaktorovej autentifikácie alebo VPN, aby zabránili ďalšiemu zneužívaniu kamier na vojenskú špionáž.vateľský reťazec.

Ruskí útočníci zneužívajú zero-click zraniteľnosť v Zimbre na krádež e-mailov

CISA spolu s partnermi upozornila, že ruská štátom podporovaná skupina Laundry Bear (Void Blizzard) aktívne zneužíva zraniteľnosť CVE-2025-66376 v aplikácii Zimbra Collaboration na krádež e-mailov, prihlasovacích údajov a obnovovacích kódov dvojfaktorovej autentifikácie. Útok využíva uloženú XSS zraniteľnosť v rozhraní Classic Web Client. Škodlivý JavaScript sa spustí už pri zobrazení e-mailu. Kampaň zasiahla organizácie na Ukrajine, v USA a vo viacerých členských štátoch NATO vrátane Českej republiky. Organizáciám, ktoré využívajú aplikáciu Zimbra, sa odporúča nasadiť dostupné bezpečnostné aktualizácie.

VÝZNAMNÉ UDALOSTI VO SVETE



CERT-UA varuje pred kampaňou zneužívajúcou Notepad++

Ukrajinský tím CERT-UA upozornil na kampaň skupiny UAC-0099, ktorá šíri archív obsahujúci legitímnu aplikáciu Notepad++ spolu so škodlivou knižnicou NppExport.dll a ďalšími komponentmi vrátane nástroja LunchPoke. Útočníci nevyužívajú zraniteľnosť ani kompromitáciu dodávateľského reťazca Notepad++, ale zneužívajú dôveru používateľov v legitímny softvér. Po spustení balíka sa škodlivý modul automaticky načíta a zabezpečí perzistenciu v systéme. Kampaň je pripisovaná skupine UAC-0099, ktorá podľa CERT-UA poskytuje počiatočný prístup pre útoky skupiny APT44 (Sandworm) zamerané najmä na organizácie na Ukrajine.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

DirtyClone: zraniteľnosť jadra Linuxu umožňuje získať práva root

V jadre operačných systémov Linux bola opravená vysoko závažná zraniteľnosť, ktorá umožňuje lokálnym útočníkom s nízkymi oprávneniami vykonávať zmeny v pamäte pomocou klonovaných sieťových paketov a získať oprávnenia používateľa root. Chyba zabezpečenia patrí do sady chýb DirtyFrag a dostala názov DirtyClone.

Januscape: zraniteľnosť Linuxového hypervízora KVM

Hypervízor KVM pre Linux obsahuje zraniteľnosť, ktorá útočníkom s prístupom ku vitruálnemu stroju a s oprávneniami používateľa root umožňuje spôsobiť kernel panic na hostiteľovi (DoS), a v istých prípadoch tiež na hostiteľovi vykonávať kód s oprávneniami root. Zraniteľné sú najmä multi-tenantné cloudové systémy s vnorenou virtualizáciou.

Routery Tenda obsahujú zadné vrátka do administrátorského rozhrania

Tím CERT/CC objavil zadné vrátka vo firmvéri smerovačov Tenda, ktoré umožňujú zadať alternatívne predkonfigurované heslo bez znalosti používateľského mena, a získať administrátorský prístup ku zariadeniu. Táto funkcia nie je zdokumentovaná, ani viditeľná v administrátorskom rozhraní.

Ubiquiti opravila kritické zraniteľnosti v UniFi Connect, UniFi Talk, UniFi Access, UniFi Protect a UniFi OS

Spoločnosť Ubiquiti vydala bezpečnostné aktualizácie, ktoré riešia 25 kritických a vysoko závažných bezpečnostných zraniteľností ovplyvňujúcich UniFi Connect, UniFi Talk, UniFi Access, UniFi Protect a UniFi OS. Kritické chyby umožňujú eskaláciu privilégií a vykonávanie ľubovoľných príkazov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť Zimbra Classic Web Client

Vývojári mailového klienta Zimbra Classic Web Client opravili kritickú chybu, ktorá umožňuje vykonávať útoky typu XSS a týmto spôsobom vykonávať kód v zariadení obetí.

Kritické zraniteľnosti rozšírení Joomla, iCagenda a Balbooa Forms, umožňujú vykonávať kód

Vývojári rozšírení iCagenda a Balbooa Forms pre redakčný systém Joomla opravili kritické zraniteľnosti, ktoré umožňujú nahrávať na webserver súbory s ľubovoľnými príponami, čo môže viesť ku vzdialenému vykonaniu kódu PHP, alebo iného kódu pod kontrolou útočníka.

Zraniteľnosti RabbitMQ umožňujú získavať informácie a administrátorský token

Vývojári message brokera RabbitMQ opravili dve zraniteľnosti, ktoré umožňujú neautentifikovaným útočníkom získať klientske tajomstvo OAuth a cez neho administrátorský token, alebo vykonávať zber informácií o prebiehajúcej komunikácii.

SAP opravil v júli kritické zraniteľnosti v NetWeaver, Approuter a Commerce Cloud

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoj produkt Backup & Replication, ktoré opravujú kritickú zraniteľnosť. CVE-2026-44963 umožňuje doménovému používateľovi vzdialené vykonanie kódu na zálohovacom serveri.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zneužívaná kritická zraniteľnosť Oracle EBS Payments

Spoločnosť Oracle opravila kritickú zraniteľnosť v aplikácii Oracle Payments, ktorá je súčasťou E-Business Suite. Neautentifikovaný útočník ju môže zneužiť pre získanie kontroly nad aplikáciou. Zraniteľnosť je aktívne zneužívaná.

WP2shell: zraniteľnosti jadra WordPress umožňujú vykonávať kód

V jadre redakčného systému WordPress boli opravené dve zraniteľnosti, ktoré po zreťazení umožňujú vzdialene vykonávať kód bez potreby autentifikácie. Existuje pre ne verejne dostupný exploit. Zraniteľnosti dostali spoločný názov wp2shell.

Zraniteľnosti produktov Zoom pre Windows umožňujú navýšiť oprávnenia a prevziať účty

Spoločnosť Zoom vydala aktualizácie pre kritickú zraniteľnosť v Zoom Workplace pre Windows. CVE-2026-53412 môže neautentifikovanému útočníkovi umožniť prevziať používateľský účet. Zároveň opravila tri vysoko závažné zraniteľnosti, ktoré umožňujú získať vyššie oprávnenia a zasahujú niektoré ďalšie produkty.

Kritická zraniteľnosť F5 NGINX Plus a NGINX Open Source umožňuje vykonávať kód

Spoločnosť F5 opravila kritickú zraniteľnosť v produktoch NGINX Plus a NGINX Open Source, ktorá umožňuje vzdialeným neautentifikovaným útočníkom pomocou HTTP dopytov získavať informácie o ukazovateľoch v pamäti a vykonávať tak kód, alebo spôsobiť reštart systému.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť OpenSSL umožňuje efektívne vyčerpať pamäť servera

Vývojári knižnice OpenSSL opravili závažnú zraniteľnosť, ktorá umožňuje zahltiť pamäť servera odosielaním hlavičiek TLS handshake o veľkosti 11B s požiadavkou alokovať až 131KB. Chyba vyplýva za spôsobu, akým OpenSSL spracúva požiadavky na alokovanie pamäte pre telá správ.

V jadre Linuxu bolo opravených 442 zraniteľností

Vývojári linuxového jadra opravili v novej verzii 442 zraniteľností, z ktorých 57 dostalo hodnotenie kritická a 211 vysoko závažná. Zraniteľnosti ovplyvňovali správu sietí, narábanie so súborovým systémom a pamäťou, Bluetooth, virtualizáciu, ovládače a bezpečnostné prvky.

Zraniteľnosť 7-Zip umožňuje vykonávať ľubovoľný kód

Vývojári populárneho archivátora 7-Zip opravili vysoko závažnú zraniteľnosť vo funkcionalite pre narábanie s archívmi XZ. Chyba zabezpečenia umožňuje neautorizovaným útočníkom podvrhnúť obeti špeciálne upravený súbor, po ktorého otvorení dôjde ku vykonaniu ľubovoľného kódu.

V Zimbra Collaboration Suite bolo opravených deväť kritických zraniteľností

Vývojári Zimbra Collaboration Suite opravili 9 kritických zraniteľností, ktoré umožňujú vzdialene vykonávať príkazy cez útoky XSS alebo zneužitím implementácie SNMP. Jedna zraniteľnosť umožňuje obísť reštrikcie preposielania e-mailov. Ďalšie súvisia s chybami v kontrole oprávnení a autentifikácie.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť snapd v Ubuntu umožňuje získať oprávnenia root

Vývojári Ubuntu opravili vysoko závažnú zraniteľnosť v komponente snap-confine aplikácie snapd, ktorá umožňuje lokálnemu útočníkovi s nízkymi oprávneniami získať oprávnenia používateľa root.

MESAČNÍK ZRANITEĽNOSTÍ JÚL 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/4002.html