CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

AUGUST 2026

TLP: CLEAR

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

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

1 APT28 nasadzuje zadné vrátka HOOKEDGE cielené na vládne inštitúcie a diplomatov v Európe

Insikt Group zdokumentovala kampaň ruskej skupiny APT28, ktorá prostredníctvom dokumentov Word s diplomatickou tematikou napádala vládne a diplomatické organizácie v Rumunsku, Španielsku a Turecku.

2 Útočníci zneužívajú obídenie autentifikácie v Microsoft SharePoint

Zraniteľnosť CVE-2026-55040 v SharePointe útočníci zneužívajú krátko po zverejnení PoC. Agentúra CISA ju zaradila do katalógu aktívne zneužívaných zraniteľností.

3 Čínska APT skupina kompromitovala stovky serverov VMware vCenter

Spoločnosť QUIRSO zaznamenala zneužívanie kritickej zraniteľnosti CVE-2026-59310, pri ktorom útočníci kompromitovali 361 IP adries v 47 krajinách a zabezpečili si perzistentný prístup nástrojom reverse_ssh.

4 Malvér WindRelay sa vydáva za slovenské a české banky

Výskumníci zo spoločnosti Group-IB odhalili androidový malvér WindRelay, ktorý v reálnom čase prenáša NFC komunikáciu platobnej karty obete útočníkovi a zneužíva mená finančných inštitúcií v Česku, na Slovensku a v Slovinsku.

5 Útočníci ukradli z lotyšského registra vozidiel údaje 1,2 milióna ľudí

Lotyšská agentúra CSDD potvrdila cielený útok cez zraniteľný systém vystavený do internetu, pri ktorom neboli splnené viaceré povinné bezpečnostné požiadavky.

6 Útok DDOS takmer 30 hodín narúšal nórske vládne služby vrátane ID-porten

Rozsiahly útok DDoS narušil desať digitálnych služieb nórskej vlády vrátane systému elektronických receptov. Išlo už o tretí takýto útok od júna.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci august riešil typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Objavili sa tiež phishingové SMS správy s výzvou na uhradenie parkovacieho poplatku od spoločnosti EasyPark. Správa obsahovala odkaz na falošnú webovú stránku s podrobnosťami o parkovaní a realizáciou platby. Z viacerých zdrojov prijal CSIRT.SK hlásenia o pokračujúcej phishingovej kampani zneužívajúcej meno Všeobecnej zdravotnej poisťovne. Podvodné správy obsahovali rovnaký predmet: "Informácia o vašej refundácii – VšZP".

Okrem toho sa v auguste objavila nová podvodná kampaň, ktorá šírila phishingové e-maily, zvyčajne vo formáte priezvisko.meno.organizácia@outlook.com, v ktorých sa odosielateľ snažil zneužiť identitu nadriadeného pracovníka cieľovej organizácie. CSIRT.SK správy analyzoval a vydal varovanie na svojej webstránke.

V auguste kontaktovala jednotku CSIRT.SK stredná škola v jej konštituencii ohľadom podvodného mailu, ktorý bol doručený na sekretariát školy. E-mail zamestnanec otvoril a došlo k interakcii s prílohou, ktorá obsahovala škodlivý obsah. Bezpečnostné riešenie túto škodlivú aktivitu zachytilo a presunulo do karantény. Škola poskytla vzorku predmetnej správy ako aj informácie o vykonaných opatreniach. Na základe vykonanej statickej analýzy bol poskytnutý rad odporúčaní a kompletná informácia, o aký malvér sa jedná aj s popisom jeho činností.

Na základe medializovaných informácií týkajúcich sa možného narušenia bezpečnosti a dôvernosti citlivých údajov v systéme Obchodného registra SR požiadal CSIRT.SK Ministerstvo spravodlivosti SR o poskytnutie oficiálneho stanoviska k predmetnej situácii. Ministerstvo informovalo, že prebieha preverovanie predmetnej záležitosti a vyhodnocovanie zo strany príslušných útvarov. CSIRT.SK v zmysle interných postupov a na základe dostupných informácií vyhodnotil, že predmetný incident nepredstavoval kybernetický bezpečnostný incident. Narušenie dôvernosti dát bolo spôsobené nedostatočným zabezpečeným prístupu ku citlivým dátam subjektov zapísaných v Obchodnom registri. V čase analýzy webového portálu ORSR, resp. pri pokuse replikovať procesné prevedenie zobrazenia citlivých dát sa zistilo, že medializovaný stav bol realizovateľný. Webový portál ORSR umožňoval automatizované získavanie údajov bez obmedzenia frekvencie požiadaviek (rate limitu). Dokumenty s osobnými údajmi vrátane citlivých údajov boli dostupné po vyplnení CAPTCHA.

V auguste VJ CSIRT prijala informáciu o pokuse o zneužitie zraniteľnosti CVE-2026-42897 v Microsoft Exchange Server v organizácii patriacej do konštituencie VJ CSIRT. Zraniteľnosť umožňuje šírenie škodlivých špeciálne pripravených e-mailov obsahujúcich XSS exploit. Keď obeť otvorí e-mail v OWA, spustí sa útočníkov škodlivý JavaScript a nainštalujú sa perzistentné zadné vrátka. VJ CSIRT poskytla podrobnejšie informácie o zraniteľnosti, rad odporúčaní na mitigáciu problému a požiadala o výsledky preverenia kompromitácie.

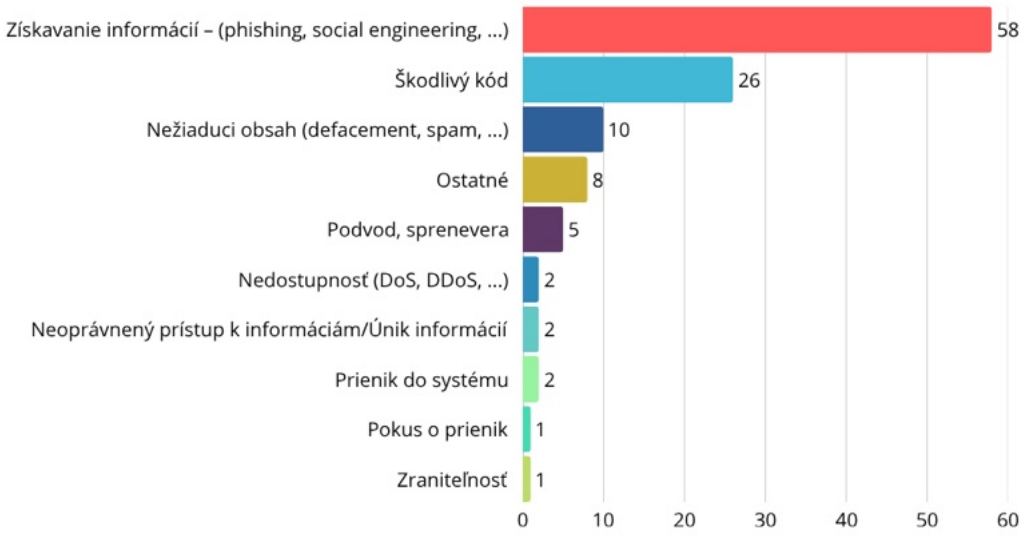
Organizácia v konštituencii VJ CSIRT požiadala o poskytnutie odporúčaní na zamedzenie zmeny obsahu na svojej webovej stránke. Časť pôvodného obsahu zmenil neznámy útočník na informácie o online kasíne. Poskytovatelia hostingu nemali vedomosť, ako k predmetnej kompromitácii došlo. Na základe poskytnutých informácií jednotka zaslala návrh súboru opatrení na zamedzenie opätovnej kompromitácie webovej stránky. V podobných prípadoch je dôležité dbať na to, akou formou bude vykonaná obnova stránky, aby nedošlo k opätovnému vneseniu počiatočnej zraniteľnosti do aplikácie, a teda umožneniu opakovanej kompromitácie.

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).

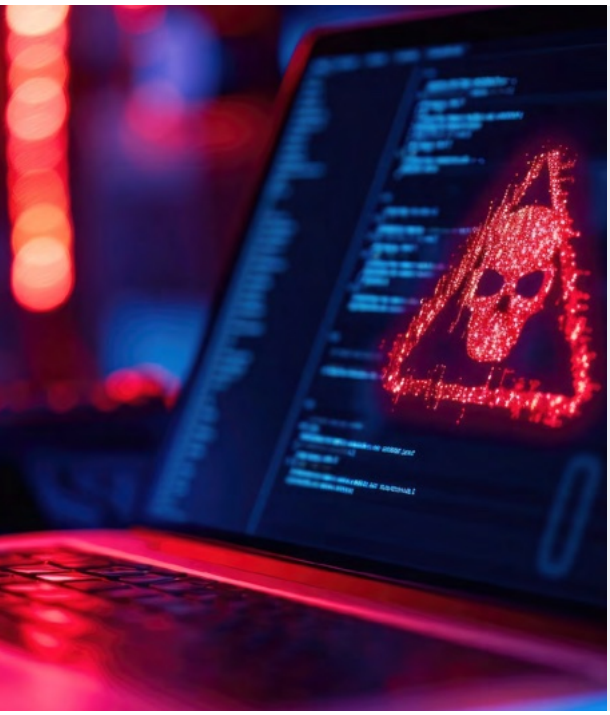
V rámci služby Ares boli vykonané penetračné testy piatich webových aplikácií a infraštruktúry jednej organizácie. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

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 auguste jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti učiteľom Strednej odbornej školy dopravy a služieb v Nových Zámkoch.

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



VÝZNAMNÉ UDALOSTI VO SVETE



Skupina APT28 cieli na vládne a diplomatické organizácie v Európe novými zadnými vrátkami HOOKEDGE

Insikt Group spoločnosti Recorded Future zdokumentovala kampaň ruskej skupiny BlueDelta (APT28), ktorá od konca septembra 2025 do začiatku apríla 2026 cielila na vládne a diplomatické organizácie v Rumunsku, Španielsku a Turecku. Operátori doručovali malvér prostredníctvom cieleného phishingu so škodlivými dokumentmi Microsoft Word s diplomatickou tematikou, pričom prvé verzie napodobňovali materiály španielskej vlády. Nasadzované zadné vrátka HOOKEDGE sú skript pre Windows, ktorý sťahuje príkazy zo služby webhook.site. Tieto vykonáva a výsledky odosiela cez skryté inštancie prehliadača Microsoft Edge. Výskumníci ho považujú za priameho nástupcu malvéru HEADLACE a upozorňujú na jeho priebežné upravovanie s cieľom obísť sandboxové analýzy.

Útočníci zneužívajú zraniteľnosť Microsoft SharePoint krátko po zverejnení PoC exploitu

Spoločnosť Defused zaznamenala útoky na zraniteľnosť CVE-2026-55040 v Microsoft SharePoint, ktoré začali 12. augusta 2026, deň po tom, čo spoločnosť Rapid7 zverejnila technické detaily a ukážku jej zneužitia. Zraniteľnosť umožňuje neautentifikovanému útočníkovi obísť overenie tokenu JWT a vykonávať operácie v mene používateľov alebo administrátorov stránky. Microsoft ju opravil v rámci júlových aktualizácií. Organizácia CISA ju 18. augusta 2026 zaradila do katalógu aktívne zneužívaných zraniteľností. Útočníci následne skúšali reťazenie so zraniteľnosťou CVE-2026-63520 v Business Connectivity Services s cieľom dosiahnuť vzdialené vykonanie kódu.

Čínska APT skupina zneužíva kritickú zraniteľnosť VMware vCenter na nasadenie zadných vrátok

Nemecká spoločnosť QUIRSO zaznamenala, že útočníci zneužívajú kritickú zraniteľnosť CVE-2026-59310 (CVSS 9,8) päť dní po jej zverejnení. Chyba zabezpečenia, ktorú spoločnosť Broadcom opravila v júli 2026, umožňuje prechádzanie ciest vo VMware vCenter Server. Útočníci po vzdialenom vykonaní kódu nasadzujú škodlivý cron job s open-source nástrojom reverse_ssh, ktorý cez odchádzajúce spojenie obchádza ochrany prichádzajúcej prevádzky. Kampaň zasiahla 361 unikátnych IP adries v 47 krajinách, najviac v Nemecku, USA, Turecku, Iráne a vo Francúzsku, a je pripisovaná aktérovi APT s podozrením na väzbu na Čínu. CISA zaradila zraniteľnosť 18. augusta 2026 do katalógu aktívne zneužívaných zraniteľností.

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

VÝZNAMNÉ UDALOSTI VO SVETE

Približne 30-hodinový DDoS útok ochromil digitálne služby nórskej vlády

Rozsiahly útok DDoS narušil približne na 30 hodín desať digitálnych služieb nórskej vlády vrátane systému ID-porten, ktorý na overovanie identity pri prístupe k verejným službám používa viac ako 4,5 milióna ľudí. Výpadok zasiahol aj systém elektronických receptov, výmenu dát medzi úradmi, prístup k verejným registrom a časť zdravotníckych služieb. Útok smeroval na infraštruktúru spoločnosti Vivicta, IT partnera nórskej agentúry pre digitalizáciu Digdir. Ide o tretí podobný incident od júna 2026, pričom táto vlna bola podľa Digdir dva až trikrát silnejšia než predchádzajúca. Útočníci sa k citlivým údajom nedostali a pôvodca útoku zatiaľ nie je známy.

Prebieha kampaň zneužívajúca kritickú zraniteľnosť v Zimbra Collaboration Suite

CERT Polska upozorňuje na prebiehajúcu kampaň, ktorá zneužíva zraniteľnosť CVE-2026-73570 umožňujúcu vkladanie systémových príkazov v Zimbra Collaboration Suite. Zraniteľnosť umožňuje neautentizovanému útočníkovi vykonať ľubovoľné príkazy s oprávneniami používateľa zimbra na inštanciách so zapnutou službou SNMP trap (parameter snmp_notify) a bežiacou službou swatchdog, ktorá je predvolene zapnutá. Francúzsky CERT-FR potvrdil, že podľa agentúry ENISA je zraniteľnosť aktívne zneužívaná. Oprava je dostupná vo verzii 10.1.20. Administrátorom sa odporúča bezodkladne aktualizovať, preveriť záznamy v /var/log/zimbra.log a skontrolovať súbory vytvorené používateľom zimbra za posledných 30 dní v adresároch webových aplikácií a v /tmp.

Zraniteľnosť v Citrix NetScaler umožňuje vzdialené vykonanie kódu a útočníci ju už zneužívajú

Útočníci zneužívajú zraniteľnosť CVE-2026-8452 typu memory overflow v Citrix NetScaler ADC a NetScaler Gateway, ktorú Citrix opravil 30. júna 2026 a pôvodne ju opísal ako chybu spôsobujúcu odopretie služby. Výskumníci zo spoločnosti watchTowr 14. augusta 2026 ukázali, že umožňuje aj neautentifikované vzdialené vykonanie kódu na zariadeniach nakonfigurovaných ako brána (SSL VPN, ICA Proxy, CVPN, RDP Proxy) alebo AAA virtuálny server. Spoločnosti Defused a Previdian následne pozorovali útoky, pri ktorých útočníci nasadzovali webshelly. CISA zaradila zraniteľnosť 26. augusta 2026 do katalógu aktívne zneužívaných zraniteľností. Administrátorom sa odporúča aktualizovať na verzie 14.1-72.61, 13.1-63.18 alebo 13.1-37.272.

VÝZNAMNÉ UDALOSTI VO SVETE

Čínski aktéri zneužívajú kritickú zraniteľnosť v Oracle HTTP Server a WebLogic Proxy Plug-in

Organizácia CISA zaradila zraniteľnosť CVE-2026-21962 (CVSS 10,0) v Oracle HTTP Server a Oracle WebLogic Server Proxy Plug-in do katalógu aktívne zneužívaných zraniteľností. Chyba v riadení prístupu umožňuje neautentifikovanému útočníkovi cez HTTP vytvárať, mazať alebo upravovať kritické dáta. Zneužívanie potvrdili spoločnosti GreyNoise, CloudSEK a SOCRadar, pričom aktéri s väzbou na Čínu ju využili pri útokoch vo viac ako 100 krajinách na doručenie downloadera SNOWLIGHT, často v kombinácii so staršími zraniteľnosťami WebLogic. Spoločnosť Oracle zraniteľnosť opravila už v januári 2026, preto sa odporúča bezodkladne overiť nasadenie januárovej aktualizácie.

Ransomvér Gunra zneužíva zraniteľnosti FortiOS na útoky proti vládnym organizáciám a kritickej infraštruktúre

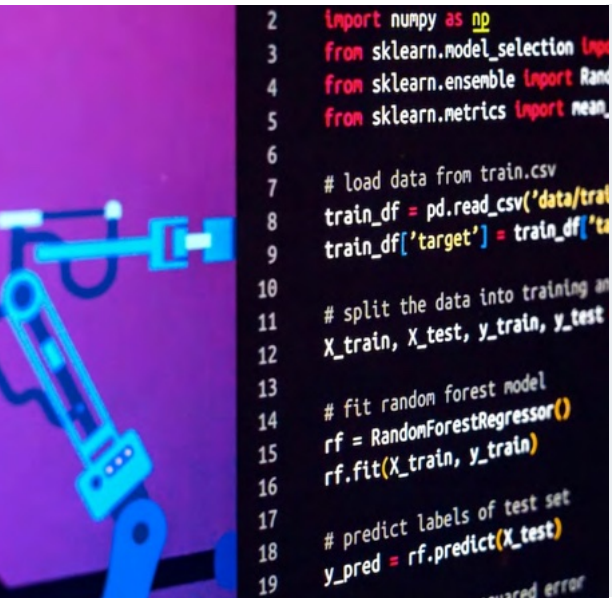
FBI, CISA a partnerské agentúry varujú pred ransomvérovou skupinou Gunra, ktorá prevádzkuje službu ransomware-as-a-service a na počiatočný prístup zneužíva zraniteľnosti obídenia autentifikácie CVE-2024-55591 a CVE-2025-24472 v produktoch FortiOS a FortiProxy. Skupina zasiahla organizácie zo sektorov zdravotníctva, financií, verejnej správy a kritickej infraštruktúry, okrem iného v Turecku, na Taiwane, v USA, Južnej Kórei, Brazílii, Japonsku a Kanade. Podľa spoločného upozornenia AA26-222A útočníci konajú prevažne medzi 22:00 a 6:00 miestneho času obete, keď sú administrátori mimo práce. Agentúry odporúčajú prednostne opraviť systémy vystavené do internetu, zabezpečiť VPN a RDP viacfaktorovou autentifikáciou, segmentovať sieť a udržiavať offline nemenné zálohy.

Skupina Lazarus zneužila Winows zraniteľnosť proti obrannému a leteckému priemyslu

Výskumníci zo spoločnosti Check Point zdokumentovali novú vlnu kampane Operation Dream Job severokórejskej skupiny Lazarus, ktorá prostredníctvom falošných pracovných ponúk cielila na obranné a letecké spoločnosti vo Francúzsku, v Nemecku, Brazílii a Indii. Na eskaláciu oprávnení na úroveň SYSTEM skupina zneužívala zero-day zraniteľnosť CVE-2026-68820 (CVSS 7,0) typu use-after-free v ovládači AFD.sys, ktorú Microsoft opravil v rámci augustových aktualizácií. Ako vstupný vektor slúžili weby imitujúce spoločnosť Enveil, ktoré šírili upravený PDF prehliadač SecurityPDF doručujúci downloader MISTPEN. Ten následne nasadzoval rootkit FudModule a zadné vrátka Troy so 17 príkazmi. V jednom prípade útočníci zneužili kompromitovanú francúzsku organizáciu na ďalší spear-phishing a na napadnutých serveroch Roundcube nasadili PHP webshell RelayShell.

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

VÝZNAMNÉ UDALOSTI VO SVETE

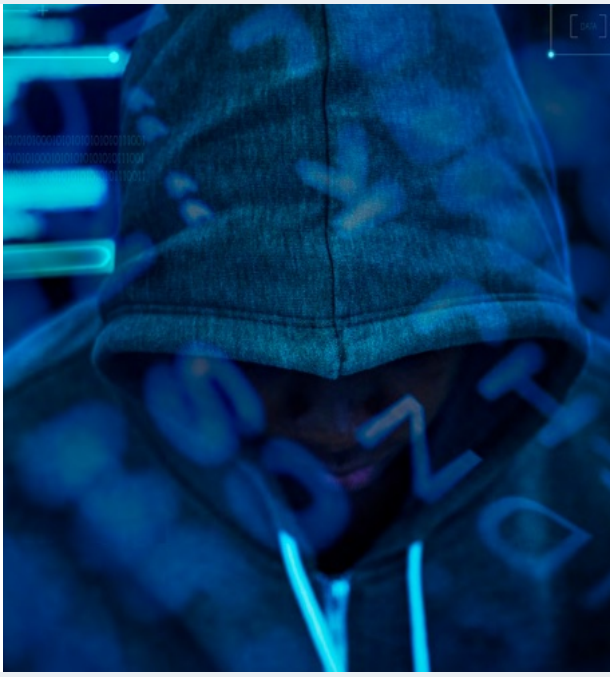


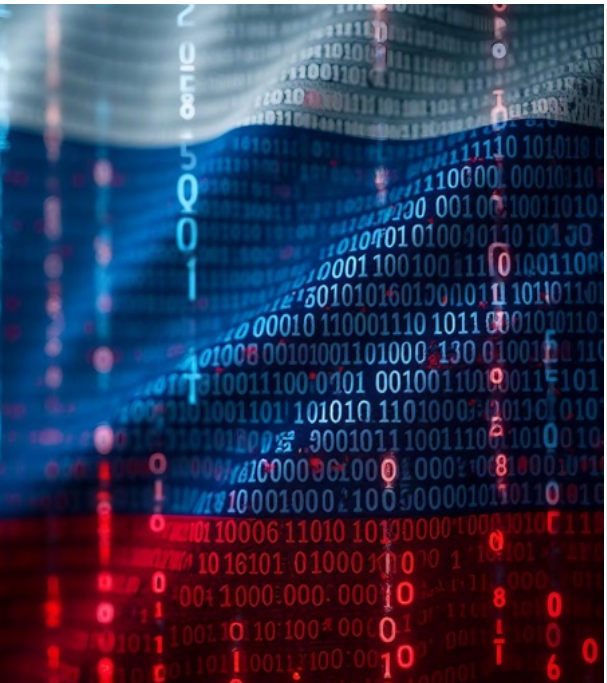
Útočníci zneužívajú kritickú zraniteľnosť GitLab dva dni po jej zverejnení

Spoločnosť watchTowr zaznamenala pokusy o zneužitie kritickej zraniteľnosti CVE-2026-19478 (CVSS 9,4) v GitLab CE/EE približne dva dni po vydaní opravy 17. augusta 2026. Zraniteľnosť typu code injection cez GraphQL direktívu umožňuje neautentizovanému útočníkovi jedinou HTTP požiadavkou upravovať alebo mazať verejné projekty a používateľské dáta, podvrhnúť záznamy o zlúčení, vymazať repozitáre či zablokovať správcov. Používateľom self-hosted inštalácií sa odporúča bezodkladne aktualizovať na verziu 19.2.4, 19.1.6, 19.0.8 alebo 18.11.11. Pokusy o zneužitie možno odhaliť vyhľadaním reťazca „@gl_introduced“ vo webových záznamoch.

Sandworm sa vydáva za náborárov a cieli na ukrajinských IT administrátorov

CERT-UA zaznamenal kampaň skupiny Sandworm (APT44, Seashell Blizzard) prepojenej s ruskou vojenskou spravodajskou službou GRU, ktorá prebieha aspoň od mája 2026 a cieli na ukrajinských systémových administrátorov a IT špecialistov. Útočníci vyhľadávajú kandidátov na legitímnych pracovných portáloch, kde vystupujú ako spoločnosť Atlas Business Group údajne hľadajúca ľudí pre Sopra Steria Bulgaria. Komunikácia pokračuje cez Telegram a pohovor cez Zoom, po ktorom je kandidát vyzvaný pripojiť sa na firemnú sieť cez VPN. Pri nahlásených problémoch dostane odkaz na aplikáciu SopraVPN, upravenú verziu open-source klienta WireGuard, ktorá umožňuje skryté vykonávanie príkazov, pričom niektoré príkazy sú zašifrované v konfiguračných súboroch VPN.





Ruská kampaň Matrioška cieli na septembrové krajinské voľby v Nemecku

Nemecké bezpečnostné orgány zaznamenali ruskú dezinformačnú kampaň Matrioška zameranú na septembrové krajinské voľby v Sasku-Anhaltsku, Meklenbursku-Prednom Pomoransku a v Berlíne. Kampaň šíri najmä na sieti X falošné príspevky a upravené videá s logami dôveryhodných médií, napríklad ARD a BBC, s vymyslenými obvineniami miestnych politikov zo sprenevery či sexuálnych trestných činov, pričom čoraz viac využíva umelú inteligenciu na tvorbu zavádzajúceho obsahu. Dosah kampane je zatiaľ obmedzený, úrady ju však považujú za súčasť ruskej hybridnej vojny s cieľom polarizovať spoločnosť. Podľa analýzy portálu Eunews kampaň diskredituje kandidátov iných strán než AfD a na rozdiel od siete Storm-1516 zatiaľ nebola jednoznačne prepojená s konkrétnou ruskou inštitúciou.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť umožňuje čítanie obsahu súborov s potenciálom vzdialeného vykonania kódu

V komponente Active Storage nástroja Ruby on Rails bola opravená kritická zraniteľnosť CVE-2026-66066, ktorá umožňuje neautentifikovanému útočníkovi čítať ľubovoľné súbory zo servera prostredníctvom špeciálne vytvoreného obrázka. Získané citlivé údaje, napríklad kryptografické kľúče, prihlasovacie údaje k databázam alebo kľúče k API, môžu následne umožniť kompromitáciu aplikácie alebo v určitých prípadoch viesť až k vzdialenému vykonaniu kódu.

Kritické zraniteľnosti VMware vCenter

Spoločnosť Broadcom opravila v produkte VMware vCenter dve kritické zraniteľnosti, z ktorých jedna je aktívne zneužívaná. Zraniteľnosti umožňujú vzdialeným neautentifikovaným útočníkom obchádzať autentifikáciu a traverzovať adresármi s cieľom vykonávania ľubovoľného kódu.

Zraniteľnosť FortiWeb umožňuje prihlásiť sa ľubovoľnými údajmi

Spoločnosť Fortinet opravila kritickú zraniteľnosť vo svojom produkte FortiWeb, ktorá umožňuje vzdialenému útočníkovi prihlásiť sa do administrátorskej konzoly s použitím ľubovoľného prihlasovacieho mena a hesla.

Zraniteľnosti GitLab CE/EE dovoľujú upravovať a meniť projekty a dáta

Vývojári platformy GitLab CE/EE opravili dve zraniteľnosti v komponente GraphQL, ktoré umožňujú vzdialeným neautentifikovaným útočníkom meniť a mazať verejné projekty a používateľské dáta.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť Red Hat build of Keycloak umožňuje prevzatie účtov

Spoločnosť Red Hat opravila kritickú zraniteľnosť v komponente keycloak-services. Chyba v procese obnovy prihlasovacích údajov umožňuje neautentizovanému útočníkovi s prístupom k službe vynútiť reset hesla ktoréhokoľvek používateľa bez nutnosti kliknúť na overovací e-mailový odkaz a získať tak plnú kontrolu nad jeho účtom.

Zraniteľnosť WordPress Elementor Pro umožňuje vykonávať kód

Vývojári modulu Elementor Pro pre WordPress opravili kritickú zraniteľnosť, ktorá dovoľuje obchádzať kontrolu zakázaných súborov a nahrávať ich na server. Vzdialený neautentifikovaný útočník tak môže získať schopnosť vykonávať ľubovoľný kód.

Oracle vydala balík záplat na 943 zraniteľností viacerých produktov

V augustovom balíku záplat opravila spoločnosť Oracle vo svojich produktoch 943 zraniteľností, vrátane 154 kritických.

V Next.js opravili dve kritické zraniteľnosti

Vývojári frameworku Next.js opravili dve kritické zraniteľnosti, ktoré umožňujú neautentifikovaným útočníkom vzdialené vykonávanie kódu.

MESAČNÍK ZRANITEĽNOSTÍ AUGUST

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/4049.html