

MESAČNÁ SPRÁVA

SEPTEMBER 2026

TLP: CLEAR





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

1

Čínsky hovoriaci útočník ukradol dáta z 27 routerov na Slovensku

Spoločnosť [GreyNoise](#) zdokumentovala kampaň aktéra označovaného ako Kapibala, ktorý zneužitím zraniteľnosti CVE-2026-7273 exfiltraval konfigurácie a hashe prihlasovacích údajov z 996 routerov Zyxel GS1900 v 48 krajinách.

2

Citrix opravil dve zero-day zraniteľnosti v NetScaler ADC a Gateway

Spoločnosť Citrix [potvrdila aktívne zneužívanie zraniteľností](#) CVE-2026-88771 a CVE-2026-88772 (obe CVSS 9.5) ešte pred vydaním opravy 27. septembra 2026. Útočníci pri nich získavali oprávnenia root a nasadzovali webshelly.

3

APT Sandworm a ransomvér Qilin zneužívajú Cisco Secure Firewall Management Centre

Tím [Cisco Talos](#) zaznamenal tri kampane zneužívajúce zraniteľnosti CVE-2026-20079 (CVSS 10.0) a CVE-2026-20316, pri ktorých útočníci nasadzovali webshelly, ransomvér Qilin a malvér Cyclops Blink spájaný so skupinou Sandworm.

4

Berlín odmietol zaplatiť výkupné po krádeži 5,79 TB úradných dát

Ransomvérová skupina Rhysida ukradla z berlínskej vládnej siete 5,79 TB administratívnych dát vrátane 46 500 zmlúv a osobných údajov vyše 12 000 osôb. [Berlín odmietol zaplatiť výkupné](#) a zasiahnuté ministerstvá odpojil od siete.

5

Cisco Identity Service Engine má zraniteľnosť s najvyšším možným skóre

Spoločnosť Cisco opravila v produktoch Identity Services Engine a ISE Passive Identity Connector [kritickú zraniteľnosť](#) CVE-2026-76460 (CVSS 10.0, CWE-648), ktorá neautentizovanému vzdialenému útočníkovi umožňuje zaslaním upravenej požiadavky obísť prihlásenie do webového správcovského rozhrania..

6

Ruské špionážne skupiny automatizovali celý útočný reťazec pomocou umelej inteligencie

Spoločnosť [Anthropic](#) opísala skupiny [GTG-20006](#) a [GTG-50014](#), ktoré pomocou AI agentov vyvíjali malvér, testovali ho proti EDR riešeniam a autonómne ho upravovali až do úspešného obídienia ochrán pri cieľoch na Ukrajine a v Európe.

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. Pokračovala podvodná e-mailová kampaň, v ktorej sa odosielateľ snažil zneužiť identitu nadriadeného pracovníka cieľovej organizácie. Adresy odosielateľa boli vo formáte priezvisko.meno.organizacia@outlook.com. CSIRT.SK správy analyzoval a minulý mesiac vydal [varovanie](#) na svojej webstránke.

Jednotka CSIRT.SK prijala z viacerých zdrojov hlásenia o pokračujúcej phishingovej kampani zneužívajúcej meno Všeobecnej zdravotnej poisťovne, ktorá smerovala na jej klientov. Útočníci rozposielali phishingové e-mailové správy s predmetom "Vrátenie preplatku – potrebná autorizácia". CSIRT.SK doplnil analýzou získané indikátory kompromitácie v rámci kampane vo svojej službe Afrodita (inštancia MISP).

Organizácia v konštituencii CSIRT.SK poskytla jednotke CSIRT.SK podozrivé maily doručené na jej mailserver, na ktoré odpovedali traja používatelia. Títo boli poučení a adresy zablokované. Jednotka analyzovala poskytnuté vzorky e-mailov a požiadala správcov domény, odkiaľ boli škodlivé e-maily odoslané, o preskúmanie možnej kompromitácie e-mailových účtov na zasiahnutom serveri. Doména, z ktorej bola phishingová aktivita šírená na vládne inštitúcie v Slovenskej republike, patrila legítimnej organizácii. Zodpovední správcovia vykonali potrebné kroky k zamedzeniu tejto škodlivej aktivity.

Zaujímavé hlásenie prišlo v septembri od fyzickej osoby. Jednalo sa o pokus o podvod v spojitosti s úverom v Tatrabanke. Dotyčnú osobu kontaktoval podvodník telefonicky, pričom sa vydával za príslušníka policajného zboru. Ku koncu sa až agresívnym spôsobom pokúšal získať jej osobné údaje. CSIRT.SK získala mailovú komunikáciu s prílohami. Doména „minvpzhumenne(.).sk“, z ktorej podvodník komunikoval, napodobňovala názov a identitu služieb poskytovaných Ministerstvom vnútra Slovenskej republiky. Bola registrovaná na zahraničnú IP adresu. Nahlasovateľovi odporučila jednotka rad opatrení, okrem iného v prípade vzniku škody alebo podozrenia na trestný čin neodkladne kontaktovať najbližší útvar policajného zboru. Ak prijmete nečakaný telefonát, v ktorom sa volajúci predstaví ako príslušník polície, zamestnanec banky, alebo iná osoba s autoritou, pričom od Vás bude pod rôznymi zámienkami požadovať prevod peňazí (napríklad na „bezpečný účet“), požiadanie o úver alebo odovzdanie citlivých osobných informácií, odporúčame Vám navrhnúť, že potrebné úkony vykonáte osobne na pobočke banky alebo útvaru PZ SR, alebo s ľubovoľnou zámienkou ukončiť telefonát a pravosť situácie si overiť zavolaním na oficiálny kontakt inštitúcie, pre ktorú volajúci domnele pracuje. Získate ho napríklad z oficiálnych webstránok organizácie. Nikdy nevolajte na číslo, z ktorého ste hovor prijali, pretože toto môže byť pod kontrolou podvodníkov.

V septembri jednotka CSIRT.SK prijala od školy v Prešovskom kraji hlásenie incidentu, ktorý ilustruje dôležitosť používania dostatočne silných hesiel a správnej digitálnej hygieny všeobecne. Do portálu Edupage pod kontom zamestnanca školy sa prihlásila neznáma osoba. V jeho mene odoslala správy rodičom, žiakom a zamestnancom. Správy mali rasistický a vulgárny obsah. Správca ihneď po zistení zrušil predmetné konto a vygeneroval nové prihlasovacie údaje. Všetky správy a reakcie na ne boli vymazané a bola odoslaná ospravedlňujúca správa zasiahnutým používateľom Edupage. CSIRT.SK analyzoval predmetné správy a odporučil incident riešiť s PZ SR. Preveril tiež známe úniky prihlasovacích údajov spojené menom zasiahnutého zamestnanca, bez nálezov. Pravdepodobne teda útočník heslo uhádol alebo zlomil hrubou silou.

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).

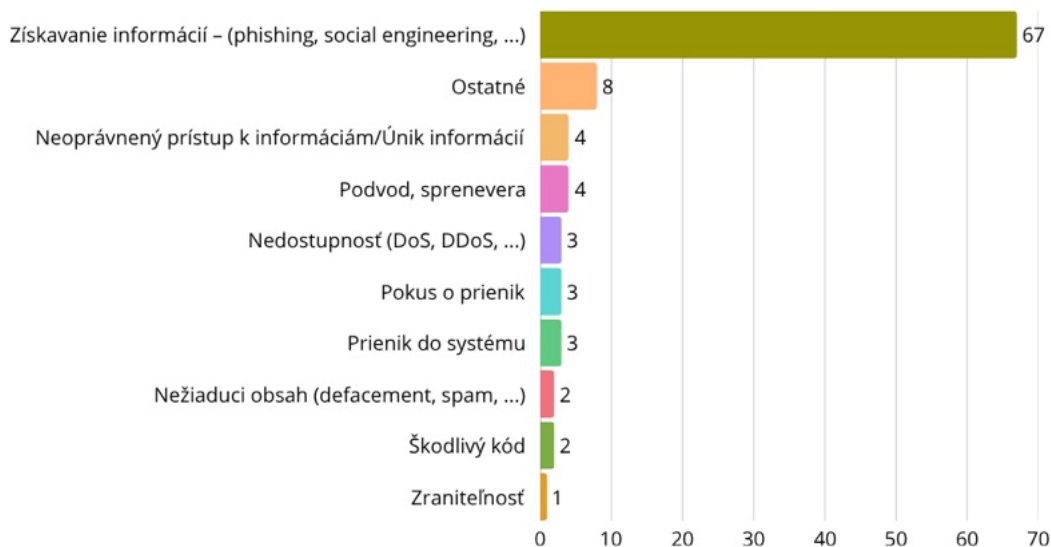
V rámci služby Ares bolo vykonaných 5 penetračných testov webových aplikácií a jeden test externej infraštruktúry štátnej organizácie.

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 septembri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti zamestnancom Štatistického úradu SR v Prešove a Košiciach. Učiteľom prednášala na Strednej priemyselnej škole elektrotechnickej v Prešove, Strednej zdravotníckej školy a Základnej školy Petra Škrabáka v Dolnom Kubíne. V septembri si prednášku CSIRT.SK vypočuli študenti Hotelovej akadémie Mikovíniho 1 v Bratislave.

Členovia tímu CSIRT.SK sa v septembri zúčastnili konferencií [KISS 2026](#) (Konferencia Informatikov Samospráv Slovenska) v Brezne a [AlfasatIT EXPO 2026](#) v Moldave nad Bodvou. Prednášali zamestnancom obcí a škôl a predstavili im služby Vládnej jednotky CSIRT, ktoré môžu bezplatne využívať pri svojej každodennej činnosti.

VJ CSIRT poskytuje tiež školenia a cvičenia pre svoju konštituenciu v rámci [výcvikového a školiaceho strediska Kyberaréna](#).



VÝZNAMNÉ UDALOSTI VO SVETE

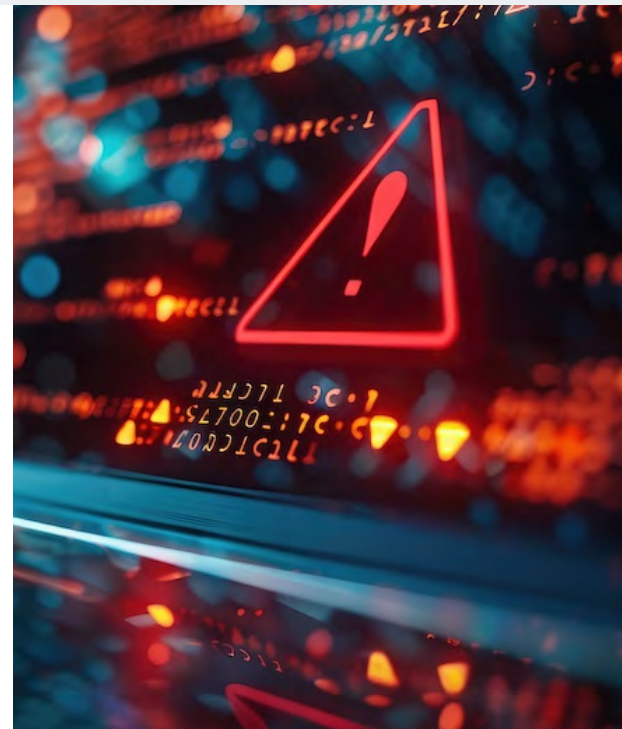


Útočník Kapibala kradol dáta cez WordPress aj routery Zyxel

Spoločnosť [GreyNoise](#) zverejnila [analýzu](#) aktivity útočníka Kapibala, pravdepodobne čínsky hovoriaceho aktéra v časovom pásme UTC+8. Od júla 2026 zneužíval reťazec zraniteľností WordPress CVE-2026-63030 a CVE-2026-60137 a kompromitoval najmenej 49 organizácií, prevažne malé podniky a orgány verejnej správy. Pri závažnom útoku na web západnej vlády útočník vytvoril skrytý administrátorský účet, získal prístup k internej SQL databáze a stiahol vyše 18 500 záznamov vrátane hesiel v čitateľnej podobe. Nedávno navyše nástrojom na zneužitie zraniteľnosti CVE-2026-7273 získal konfigurácie a hashované prihlasovacie údaje úrovne root z 996 routerov Zyxel GS1900 v 48 krajinách. Správcom sa odporúča aktualizovať WordPress aj firmvér routerov Zyxel a zmeniť prednastavené heslá.

Útočníci zneužívali zraniteľnosti Citrix NetScaler ešte pred vydaním opravy

Spoločnosť [Citrix](#) potvrdila [aktívne zneužívanie](#) dvoch kritických zraniteľností v NetScaler ADC a NetScaler Gateway. CVE-2026-88771 umožňuje spustiť príkazy bez autentifikácie a zasahuje všetky nasadenia bez ohľadu na konfiguráciu. CVE-2026-88772 vedie ku vzdialenému spusteniu kódu alebo odopretiu služby na zariadeniach s protokolom DTLS. Obe boli zneužívané ešte pred zverejnením septembrovej opravy. Útočník sa v pokuse o zneužitie zraniteľnosti voči senzoru spoločnosti GreyNoise na ňom pokúsil nastaviť bity setuid a setgid na /bin/sh s cieľom získať shell s oprávneniami používateľa root a nainštalovať heslom chránený webshell maskovaný ako skrytý súbor .ctxs.receiver. Používateľom sa odporúča bezodkladne aktualizovať a zariadenia preveriť na známky kompromitácie. Tieto zraniteľnosti boli taktiež zdokumentované v rámci služby CSIRT.SK Afroditu.



Vlastný nástroj PivotC2 slúži na dlhodobý prístup k zariadeniam FortiGate

Spoločnosť [SOCRadar](#) opísala [kampaň](#) zneužívajúcu kritickú zraniteľnosť CVE-2025-25249 (CVSS 9.8, CWE-122) v systémoch FortiOS a FortiSwitchManager. Ide o pretečenie haldy v cw_acd dostupnom na porte UDP 5246, ktoré umožňuje vzdialene spustiť kód alebo príkazy bez autentifikácie. Útočníci od júla preskenovali viac než 30 000 adries IP a 178 zariadení infikovali vlastným nástrojom PivotC2 postaveným na platforme Node.js, ktorý po prieniku zabezpečí trvalý prístup k zariadeniam. Používateľom sa odporúča ihneď aktualizovať FortiOS a FortiSwitchManager na opravenú verziu a preveriť odchádzajúcu komunikáciu na známe adresy riadiacich serverov.

VÝZNAMNÉ UDALOSTI VO SVETE



Tri rôzne kampane zneužívajú zraniteľnosti v Cisco Secure Firewall Management Center

Tím [Cisco Talos zaznamenal pokračujúce zneužívanie](#) dvoch zraniteľností v produkte Cisco Secure Firewall Management Center. CVE-2026-20079 (CVSS 10.0) umožňuje obísť autentifikáciu a získať prístup s oprávneniami root, zatiaľ čo CVE-2026-20316 využíva statické prihlasovacie údaje. Zraniteľnosti sú zneužívané v kampaniach, ktorých súčasťou je nasadzovanie webshellov, ransomvéru Qilin a malvéru Cyclops Blink spájaného so skupinou Sandworm. Keďže ide o centrálny správčový prvok bezpečnostnej infraštruktúry, jeho kompromitácia dáva útočníkovi kontrolu nad politikami ochrany celej siete. Správcom sa odporúča bezodkladne nainštalovať opravy a prístup k správčovskému rozhraniu obmedziť na vyhradený segment siete.

Rhysida ukradla berlínskej vláde 5,79 TB dát a ponúkla ich na predaj

Ransomvérová skupina Rhysida sa prihlásila k útoku na berlínske úrady, pri ktorom údajne ukradla 5,79 TB administratívnych dát vrátane zmlúv, osobných údajov, hesiel a utajovaných informácií. Tieto ponúkla v aukcii za 30 bitcoinov. [Primátor Kai Wegner potvrdil](#), že Berlín výkupné nezaplatí, preto po odmietnutí platby skupina ukradnuté dáta zverejnila. Podľa spoločného upozornenia amerických autorít skupina Rhysida ako vstupný vektor využíva uniknuté prihlasovacie údaje a po získaní prvotného prístupu používa PowerShell a príkazový riadok na sťahovanie ďalších škodlivých súborov a mapovanie hostiteľského systému. Organizáciám sa odporúča vynucovať viacfaktorové overovanie pri prístupe do podnikovej siete, obmedziť spúšťanie príkazového riadka a PowerShellu a zapnúť auditovanie jeho činnosti.



Zero-day zraniteľnosti v PaperCut NG a MF sa zneužívajú na krádež databáz

[Dve zero-day zraniteľnosti v tlačovom softvéri PaperCut](#) NG a MF, CVE-2026-81578 a CVE-2026-82078, boli zneužívané už pred vydaním opráv a dajú sa reťažiť na obídenie autentifikácie a vzdialené vykonanie kódu. Tento softvér používajú aj veľké podniky, štátne inštitúcie a vzdelávacie zariadenia. Spoločnosť Defused od konca augusta pozorovala na svojich honeypotoch útočníka, ktorý využíva obídenie autentifikácie na zneužitie externého vyhľadávania používateľov a exfiltráciu databázových tabuliek. Spoločnosť Shadowserver eviduje vyše 800 serverov PaperCut MF a NG dostupných z internetu. PaperCut vydali núdzové opravy a zverejnili indikátory kompromitácie. Organizáciám odporúčajú nainštalovať Emergency Patch Release 3 aj v prípade, že už predtým nasadili skoršiu núdzovú opravu, a tiež zrušiť verejnú dostupnosť aplikačného servera, ak nie je nevyhnutná.

VÝZNAMNÉ UDALOSTI VO SVETE



Útočníci nechali umelú inteligenciu vyvíjať malvér aj obchádzať bezpečnostné nástroje

Spoločnosť [Anthropic zverejnila septembrovú správu](#) o kybernetických hrozbách, ktorá opisuje využitie AI pri kybernetických útokoch. Skupina GTG-20006, spájaná s ruskou špiónážou, automatizovala celý útočný reťazec vrátane vývoja malvéru a krádeže dát na Ukrajine a v Európe. Agenti postavení na jazykových modeloch testovali nasadený malvér proti riešeniam EDR a autonómne upravovali kód, kým nedosiahli spoľahlivé obídenie ochrán; až potom bol nasadený v kampaniach. Ďalšia skupina, GTG-50014, napojená na ShinyHunters, využila AI na stiahnutie a dekompiláciu vyše 1,8 milióna aplikácií pre Android a na vyhľadávanie kľúčov API a citlivých údajov v ich zdrojovom kóde. Tieto následne slúžili ako vstupný bod pri ďalších operáciách.

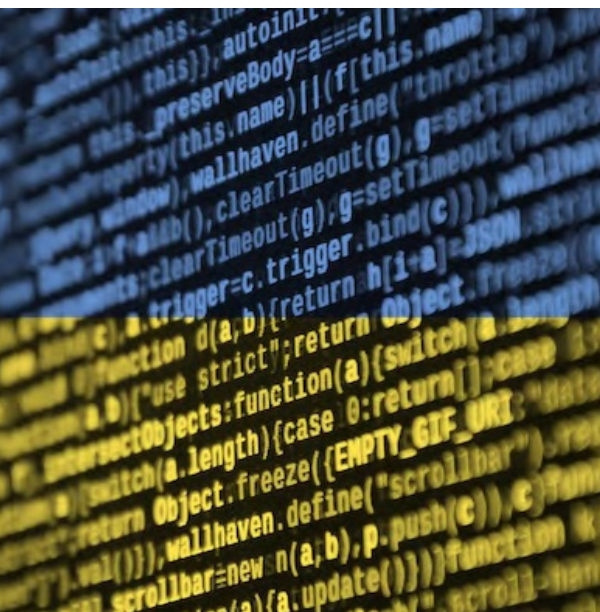
Útočníci skúšali zraniteľnosť jadra WordPressu niekoľko hodín po vydaní opravy

[V jadre systému WordPress bola opravená](#) kritická zraniteľnosť CVE-2026-87902 (CVSS 9.2, CWE-98) typu path traversal pri vyhodnocovaní šablóny stránky vo funkcii `get_page_template()`. Umožňuje neautentizovanému útočníkovi načítať ľubovoľné súbory PHP a za určitých okolností vykonať kód na serveri. Zasiiahnuté sú všetky vetvy od verzie 4.7. Oprava vyšla vo verzii 7.1.2. Spolu s ňou bola opravená aj zraniteľnosť CVE-2026-93485 (CVSS 7.1, CWE-79) typu uloženého XSS na úrovni DOM. Spoločnosť Patchstack zaznamenala prvé pokusy o zneužitie už niekoľko hodín po vydaní opravy. Aktivita počas jedného dňa prešla od overovania zraniteľnosti načítavaním súborov `.php` cez testovanie dostupnosti skriptu `pearcmd.php` až po zápis súborov `.php` s obsahom pod kontrolou útočníka do adresárov `/tmp` a `/var/tmp`. Prevádzkovateľom sa odporúča bezodkladne aktualizovať na verziu 7.1.2 alebo na zodpovedajúcu opravenú verziu svojej vetvy.



Kampaň proti Ukrajine šíri nový infostealer technikou ClickFix

[Spoločnosť Arctic Wolf opísala kampaň](#), pri ktorej útočníci napadli ukrajinské firemné weby a vložili na ne falošnú overovaciu stránku Cloudflare v ukrajinčine. Tá mala návštevníkov prinútiť spustiť škodlivý príkaz na inštaláciu malvéru. Technika ClickFix prinúti návštevníka otvoriť dialóg na spustenie programu a vykonať škodlivý príkaz. Takto doručený balík MSI inštaluje malvér typu infostealer, označovaný ako Psychedelic Stealer, ktorý kradne heslá z prehliadačov, tokeny účtov a údaje kryptomenových peňaženiek. Trvalý prístup k infikovanému zariadeniu si zabezpečuje prostredníctvom naplánovanej úlohy a komunikuje s riadiacim serverom. Odhalený riadiaci panel kampane zaznamenal aktivitu v 32 krajinách, pričom väčšina zásahov smerovala na Ukrajinu.



VÝZNAMNÉ UDALOSTI VO SVETE



Severokórejskí operátori nakazili 30 000 zariadení falošnými pracovnými pohovormi

Americké úrady vydali 17. septembra 2026 upozornenie na operáciu označovanú ako WaterPlum, v ktorej sa severokórejskí aktéri vydávajú za spoločnosti pôsobiace v oblasti umelej inteligencie a blockchainu a pod zámienkou pracovných pohovorov nútia uchádzačov sťahovať a spúšťať škodlivé súbory. Tento postup je zdokumentovaný už od roku 2024 a rovnaký modus operandi bol zaznamenaný aj proti ukrajinským odborníkom na informačné technológie. Podľa upozornenia skupina medzi decembrom 2025 a júlom 2026 infikovala najmenej 30 000 zariadení v 100 krajinách. Na zariadeniach obetí boli nájdené varianty malvéru BeaverTail, InvisibleFerret, OtterCookie, OtterCandy a StoatWaffle, pričom útočníci si udržiavali prístup s cieľom preniknúť neskôr prostredníctvom zamestnaných odborníkov aj do podnikových systémov. Kampaň je úzko prepojená s podvodnými pohovormi severokórejských pracovníkov v oblasti informačných technológií, pred ktorými dlhodobo varuje aj nemecký Spolkový úrad na ochranu ústavy.

Revolut vydal údaje zákazníkov na základe podvrhnutých žiadostí úradu

Britská spoločnosť Revolut potvrdila, že poskytla citlivé údaje zákazníkov neoprávnenej tretej strane, ktorá zaslala podvodné žiadosti o údaje z legítimnej e-mailovej domény vládnej agentúry. Útočníci využili kompromitované, no skutočné konto úradu a požiadali o núdzové poskytnutie údajov, pri ktorom sa overovanie zvykne skracovať. Uniknuté údaje zahŕňajú dátumy narodenia, poštové a e-mailové adresy a telefónne čísla, kópie dokladov totožnosti vrátane cestovných pasov a vodičských preukazov a podľa oznámenia zaslaného zákazníkom aj overovacie fotografie, výpisy z účtov a históriu transakcií. Spoločnosť po odhalení útoku kompromitované konto zablokovala a informovala príslušné orgány. Útočníci následne požadovali výkupné výmenou za nezverejnenie údajov a časť z nich napokon zverejnili. Prípade je mementom, že aj žiadosti o údaje prichádzajúce z pravých domén orgánov verejnej moci treba overovať ďalším, nezávislým kanálom.



ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV



Kritická zraniteľnosť [Cisco ISE](#) umožňuje obísť autentifikáciu

Spoločnosť Cisco opravila aktívne zneužívanú kritickú zraniteľnosť CVE-2026-76460 v produktoch Cisco ISE a ISE-PIC, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi obísť autentifikáciu prostredníctvom špeciálne vytvorenej požiadavky na rozhranie API. Spoločnosť Cisco zároveň opravila ďalších 41 kritických zraniteľností v uvedených produktoch.



Kritická zraniteľnosť [GitLab](#) umožňuje čítanie ľubovoľných súborov

Vývojári platformy GitLab opravili aktívne zneužívanú kritickú zraniteľnosť CVE-2026-85706, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi čítať ľubovoľné súbory na serveri GitLab. Súčasťou bezpečnostnej aktualizácie sú aj opravy ďalších zraniteľností umožňujúcich vykonávanie kódu, zmeny konfigurácie či narušenie dostupnosti služby.



Aktívne zneužívaná zraniteľnosť [Google Chrome](#) umožňuje vykonávanie kódu

Spoločnosť Google opravila aktívne zneužívanú zraniteľnosť CVE-2026-87491 v komponente prehliadača Chrome. Zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom špeciálne vytvorenej webovej stránky vykonávať ľubovoľný kód v izolovanom prostredí prehliadača. V rámci bezpečnostnej aktualizácie bolo opravených celkovo 230 zraniteľností, z ktorých päť bolo klasifikovaných ako kritických.



Zraniteľnosti [VMware](#) umožňujú únik z virtuálneho stroja

Spoločnosť Broadcom opravila dve závažné zraniteľnosti CVE-2026-59346 a CVE-2026-59347, ktoré umožňujú útočníkovi s oprávneniami lokálneho administrátora vykonávať ľubovoľný kód na hostiteľskom systéme. Útočník s oprávneniami lokálneho administrátora vo virtuálnom stroji môže zneužiť chyby pri spracovaní pamäte a prekročiť hranicu medzi virtuálnym strojom a hostiteľským systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV



Kritická zraniteľnosť [Red Hat](#) umožňuje získať najvyššie oprávnenia

Spoločnosť Red Hat opravila kritickú zraniteľnosť CVE-2026-18922 v komponente 389 Directory Server, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi obísť autentifikáciu a získať oprávnenia správcu adresárovej služby. Zraniteľnosť súvisí s nesprávnym spracovaním identity pri autentifikácii SASL, čo môže útočník zneužiť prostredníctvom špecifickej postupnosti autentifikačných požiadaviek. Úspešný útok môže viesť k neoprávnenému prístupu a získaniu najvyšších oprávnení v adresárovej službe.



Kritická zraniteľnosť [Cisco Nexus](#) umožňuje vzdialené vykonávanie kódu

Spoločnosť Cisco upozornila na kritickú zraniteľnosť CVE-2026-20212 v routeroch Nexus 9000 s technológiou Silicon One, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi vykonávať ľubovoľný kód s najvyššími systémovými oprávneniami. Zraniteľnosť súvisí s nedostatočne zabezpečenou sieťovou službou, ktorá spracováva vstupy bez overenia totožnosti používateľa. Úspešné zneužitie môže viesť k úplnej kompromitácii zariadenia alebo k jeho neočakávanému reštartu.

MESAČNÍK ZRANITEĽNOSTÍ SEPTEMBER 2026

VJ CSIRT pravidelne vydáva [mesačný prehľad kritických zraniteľností](https://csirt.sk/posts/4113.html).

<https://csirt.sk/posts/4113.html>