CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

OKTÓBER 2026

TLP: CLEAR





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

1 Útočníci zneužívajú zero-day zraniteľnosti Citrix NetScaler aj proti štátnej správe

Google Threat Intelligence Group upozorňuje, že útočník od septembra zneužíva zero-day zraniteľnosť CVE-2026-88772 v NetScaler ADC a Gateway na získanie oprávnení root a nasadenie webshellov v organizáciách v Severnej Amerike a Európe vrátane štátnej správy.

2 FBI a Secret Service varujú pred pokračujúcou kampaňou FortiBleed

FBI a americká Secret Service varujú, že kampaň FortiBleed kompromitovala viac ako 86 000 firewallov FortiGate. Útočníci vymknú správcov zo zariadení a prístup predávajú ransomvérovým skupinám.

3 APT Sandworm a ransomvér Qilin zraniteľností vrátane aktívne zneužívanej zero-day

Októbrový Patch Tuesday od Microsoftu opravuje 1411 zraniteľností vrátane aktívne zneužívanej CVE-2026-96951 vo Windows Shell, ktorá umožňuje obísť ochranu Mark of the Web.

4 Ruská skupina APT28 útočila na organizácie v dvoch štátoch NATO

Symantec zdokumentoval kampaň skupiny Swallowtail (APT28), spájanej s GRU, proti orgánu presadzovania práva, výrobcovi leteckých motorov a lodenici v dvoch členských štátoch NATO.

5 Kybernetický útok odstavil digitálne služby belgického ministerstva financií

Belgické federálne ministerstvo financií oznámilo kybernetický útok na svoje digitálne služby, pre ktorý preventívne odstavilo portál MyMinfin a ďalšie služby.

6 Kritickú zraniteľnosť v produktoch Atlassian útočníci zneužívajú hodiny po zverejnení POC

Zraniteľnosť CVE-2026-21589 v produktoch Atlassian Data Center umožňuje bez autentifikácie čítať súbory na serveri. Prvé pokusy o zneužitie zaznamenali výskumníci do dvoch hodín od zverejnenia PoC.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci október 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.

Opäť sa vyskytli phishingové kampane zneužívajúce mená slovenských štátnych inštitúcií. Podvodné SMS sa šírili v mene Všeobecnej zdravotnej poisťovne s odkaz na falošnú doménu imitujúcu stránku VšZP s informáciou o možnosti vrátenia preplatku. Podvodníci sa v októbri zamerali aj na Najvyšší súd SR, v ktorého mene rozposielali podvodné e-maily. Do tretice podvodníci zneužívali identitu Ministerstva práce, sociálnych vecí a rodiny SR. Rozposielali phishingové SMS správy s fotografiou a odkazom na falošnú doménu "socialna-pomoc.gov-sk[.] info/socialna_pomoc".

V rámci monitorovania kybernetických hrozieb identifikoval CSIRT.SK pomocou nástroja Recorded Future niekoľko pravdepodobne škodlivých domén pripravených na nasadenie do prevádzky, ktoré svojím vzhľadom napodobňovali webové stránky Sociálnej poisťovne. Jednotka požiadala hosting o odstránenie škodlivého obsahu.

V októbri nahlásila jednotke CSIRT.SK organizácia štátnej správy spoofing svojej e-mailovej domény. Na e-mail upozornil zamestnanec. Preverovaním sa potvrdilo, že daný e-mail neodišiel z prostredia organizácie. Obsahom e-mailu bola hrozba, že odosielateľ má prístup k osobným údajom, ktoré sprístupní na darknete, pokiaľ mu nebude uhradená požadovaná čiastka. VJ CSIRT okrem iného poukázala na odporúčania pre nasadenie overovacích a autorizačných systémov pre e-mailové servery, ktoré dokážu podobné typy útokov efektívne eliminovať.

Zamestnanci inej štátnej organizácie sa stali cieľom phishingovej kampane, ktorá šírila podvodné e-maily s predmetom „Výsledky hodnotenia pracovného výkonu zamestnancov“. CSIRT.SK požiadala hosting o odstránenie predmetnej stránky a preverila, či používatelia interagovali s doručenou správou, otvorili odkaz alebo zadali prihlasovacie údaje. Odporučila zvýšený monitoring aktivity dotknutých e-mailových účtov s cieľom odhaliť nezvyčajné pokusy o prihlásenie a blokovať IP adresy identifikované ako zdroje škodlivej aktivity.

Ďalšiu organizácie štátnej správy zasiahla vlna pokusov o SQL injection na mailovom serveri Exchange. Po vykonaní analýzy poskytnutých dát poskytla jednotka CSIRT.SK rad odporúčaní na zmiernenie incidentu. V priebehu nasledujúcich dní sa pokusy opakovali. Jednotka odporučila nastaviť na WAF filtrovanie reťazcov SQL vkladaných do poľa OWA (username, password), ako aj obmedzenie počtu požiadaviek (rate-limiting).

CSIRT.SK v rámci monitoringu hrozieb zachytil informácie o kampani s možnou väzbou na severokórejskú štátom sponzorovanú skupinu Lazarus, ktorá pripravovala celosvetové zneužívanie zraniteľností PHP2Shell v jadre PHP so zameraním na štátnu správu a finančný sektor. Kampane sa mala zúčastniť aj slovenská IP adresa. Dotyčnú organizáciu požiadal o preverenie predmetnej IP adresy a zariadenia spájaného so škodlivou infraštruktúrou. Poskytnuté dáta analyzoval.

Avšak nie každý incident je skutočne kybernetickým bezpečnostným incidentom. V rámci bezpečnostného monitoringu prijala jednotka CSIRT.SK informáciu o registrovaní veľkého množstva odmietaných požiadaviek na doménu sqm.microsoft[.]com z domény organizácie v konštituencii CSIRT.SK. Rádovo sa jednalo o 1000000

požiadaviek za 24 hod. Analýza incidentu identifikovala zodpovedný systém, ktorý zhromažďoval štatistiky o používaných aplikáciách, funkciách, chybách a výkonnostných parametroch na platforme Windows. Jednalo sa o legitímnu doménu spoločnosti Microsoft. Problém vyriešila zmena konfigurácie pre zastavenie slučky odosielania telemetrických dát.

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).

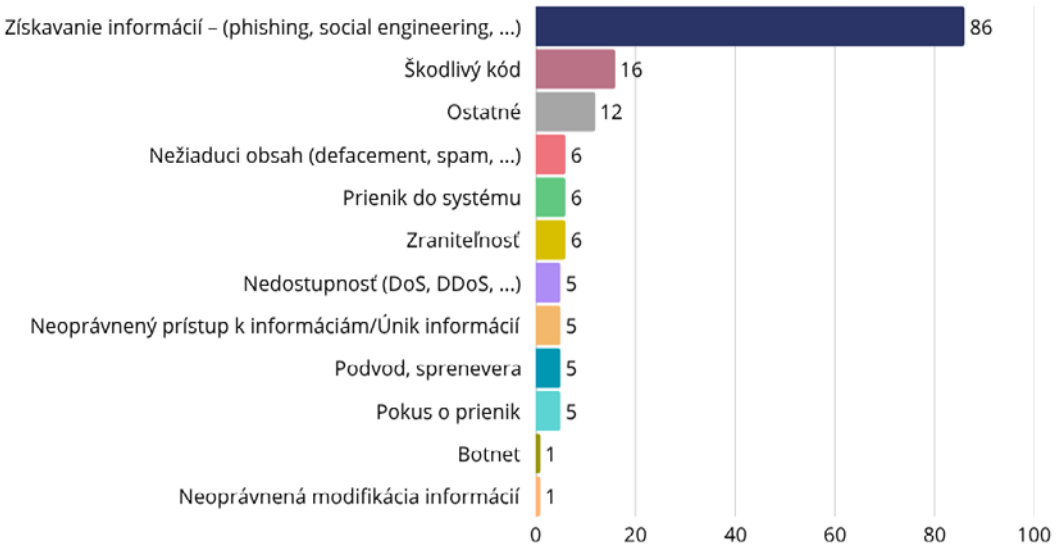
V rámci služby Ares boli vykonané 4 penetračné testy webových aplikácií. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

V októbri CSIRT.SK plošne varoval svoju konštituenciu ohľadom kritických zraniteľností CVE-2026-109618 a CVE-2026-109619 v jadre jazyka PHP, o ktorých písal aj na svojej webstránke. Informácie o nich unikli na verejnosť pred vydaním opráv. Zraniteľnosti dostali spoločný názov „php2shell“. Neautentifikovanému útočníkovi umožňujú vzdialene vykonávať ľubovoľný kód s oprávneniami webového workera.

Jednotka CSIRT.SK vydala tiež návod pre administrátorov Windowsových domén, ako efektívnejšie chrániť svoju infraštruktúru proti škodlivému kódu pomocou funkcie App Control for Business, ktorá umožňuje jednoduché nasadenie politík pre application whitelisting.

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 októbri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti zamestnancom Národného inštitútu pre hodnotu a technológie v zdravotníctve (NIHO), a tiež učiteľom Základnej školy v Miloslavove.

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



VÝZNAMNÉ UDALOSTI VO SVETE

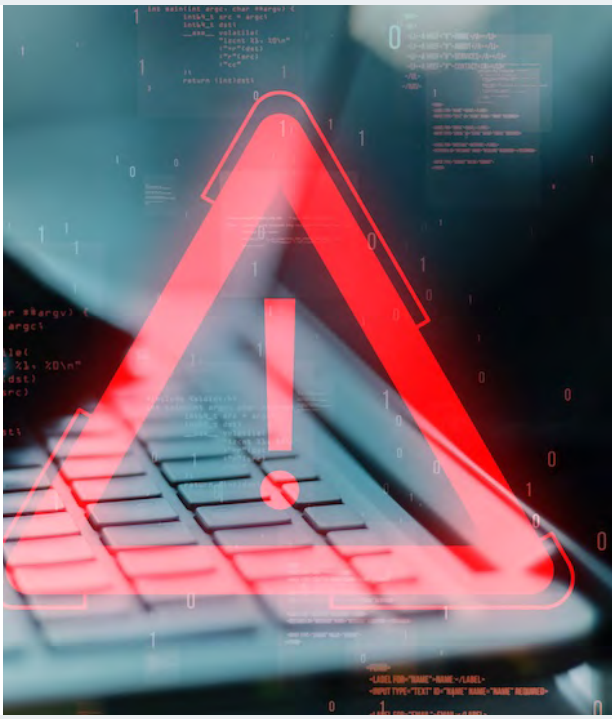


Útočníci zneužívajú zraniteľnosti v Citrix NetScaler na prienik do štátnej správy

Google Threat Intelligence Group upozorňuje, že od začiatku septembra 2026 je zneužívaná zero-day zraniteľnosť CVE-2026-88772 v zariadeniach NetScaler ADC a NetScaler Gateway. Poškodenie pamäte počas DTLS handshake umožňuje obísť autentifikáciu a získať oprávnenia root. Útočníci následne nasadzujú PHP webshelly, napríklad WHIPSHOT, ktorý skrýva komunikáciu so serverom v HTTP hlavičkách, a tunelovací nástroj SLAPSHOT na prieskum siete a krádež údajov. CERT-EU zároveň zdokumentoval zneužívanie zraniteľnosti CVE-2026-88771, ktorá umožňuje vykonávať príkazy OS cez hlavičky User-Agent. Kampaň zasiahla organizácie v Severnej Amerike a Európe v sektoroch štátnej správy, financií, technológií, školstva a právnych služieb.

Kampaň FortiBleed kompromitovala desaťtisíce firewallov a pomáha ransomvéru

FBI a americká Secret Service vydali 6. októbra 2026 spoločné upozornenie, že kampaň FortiBleed proti firewallom Fortinet FortiGate a SSL VPN dostupným z internetu stále pokračuje. SOCRadar overil viac ako 86 644 kompromitovaných zariadení v 194 krajinách. Kampaň je zdokumentovaná aj v službe CSIRT.SK Afrodita. Útočníci získavajú prihlasovacie údaje skúšaním uniknutých hesiel alebo vyťažením databázy používateľov FortiOS a offline lámaním hashov. Následne vytvárajú nové administrátorské účty, pôvodné mažú alebo im menia heslá, čím správcov vymknú zo zariadenia. Prístup potom predávajú ransomvérovým skupinám (INC/Lynx a Payload). Agentúry odporúčajú zrušiť správu zariadení z internetu, ukončiť aktívne administrátorské relácie, zmeniť heslá k VPN a správcovským účtom, zaviesť viacfaktorovú autentifikáciu odolnú voči phishingu a skontrolovať konfiguráciu, neznáme účty a kľúče REST API.





Microsoft v októbri opravil rekordných 1411 zraniteľností vrátane troch zero-day

Microsoft opravil v októbrovom Patch Tuesday rekordných 1411 zraniteľností, z toho tri zero-day. Aktívne zneužívaná je CVE-2026-96951 (CVSS 8,8) vo Windows Shell, ktorá umožňuje vloženie príkazov a sieťové obídenie ochrany Mark of the Web. Podrobnosti o útokoch Microsoft nezverejnil. Pred opravou boli verejne známe aj CVE-2026-108398 v .NET Framework, ktorá umožňuje obísť obmedzenia WDAC, a CVE-2026-92707 v knižnici MessagePack-CSharp, ktorá môže spôsobiť odopretie služby. Organizáciám sa odporúča bezodkladne nainštalovať októbrové aktualizácie pre Windows a .NET Framework, prioritne kvôli CVE-2026-96951, ktorá postihuje Windows 10, Windows 11 a Windows Server 2012 R2 až 2025.

VÝZNAMNÉ UDALOSTI VO SVETE



Ruská skupina Swallowtail útočila na bezpečnostné organizácie v dvoch štátoch NATO

Symantec Threat Hunter Team zdokumentoval kampaň ruskej špionážnej skupiny Swallowtail (známej aj ako APT28 alebo Fancy Bear), ktorá je spájaná s vojenskou spravodajskou službou GRU. Skupina cielila na organizácie v dvoch členských štátoch NATO vrátane orgánu presadzovania práva, výrobcu leteckých motorov pre armádu a lodenice, ktorá stavia námorné plavidlá. Pri útoku na lodenicu útočníci použili zadné vrátka Hookedge doručené cez dokument Word s makrom, ktoré komunikujú cez službu webhook.site. Odcudzili prihlasovacie údaje vrátane zachytenia NTLM handshake, vytvorili perzistentný SSH tunel do internej siete a nasadili doposiaľ nezdokumentovaný reflexívny loader ld.exe.

Kybernetický útok vyradil digitálne služby belgického ministerstva financií

Belgické federálne ministerstvo financií (FOD Financiën / SPF Finances) oznámilo, že čelí kybernetickému útoku na svoje digitálne služby. Portál MyMinfin a niektoré ďalšie služby preventívne odstavilo. Podľa ministerstva zatiaľ nič nenasvedčuje úniku ani krádeži údajov a väčšina aplikácií zostáva aspoň čiastočne dostupná. Na podanie vybraných daňových priznaní ministerstvo poskytne dodatočnú lehotu.



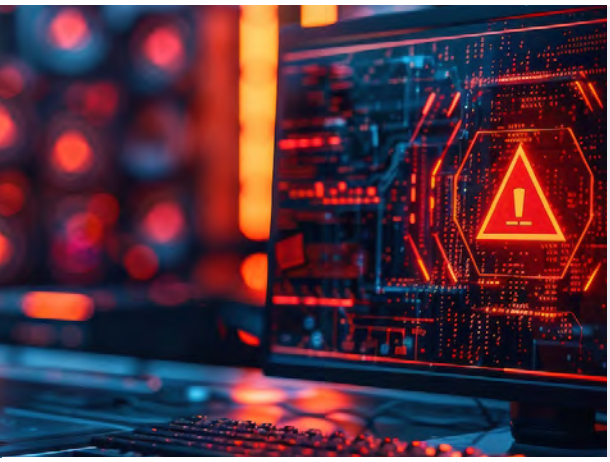


Útočníci zneužívajú kritickú zraniteľnosť v produktoch Atlassian do dvoch hodín od zverejnenia PoC

Spoločnosť Atlassian upozornila na kritickú zraniteľnosť CVE-2026-21589 (CVSS 4.0: 9,3), ktorá neautentifikovanému útočníkovi umožňuje čítať súbory v koreňovom adresári webovej aplikácie. Zasiahnuté sú lokálne spravované produkty Jira Software a Jira Service Management Data Center, Confluence, Bitbucket, Bamboo, Crowd Data Center, Crucible a Fisheye. Útoky sa začali krátko po tom, čo spoločnosť watchTowr zverejnila technickú analýzu a PoC. Ukázala v nich, že z prečítaných súborov možno v nasadeniach integrovaných s Atlassian Crowd získať prihlasovacie údaje a vytvoriť si účet administrátora Jira. Prvé pokusy o zneužitie zachytila spoločnosť Previdian vo svojej sieti honeypotov do dvoch hodín od zverejnenia. Odporúča sa bezodkladne aktualizovať na opravené verzie (napríklad Jira Software Data Center 9.12.40, 10.3.26 alebo 11.3.12). Dovtedy treba obmedziť prístup z externej siete alebo nasadiť pravidlá blokujúce prechod adresármi.

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

VÝZNAMNÉ UDALOSTI VO SVETE

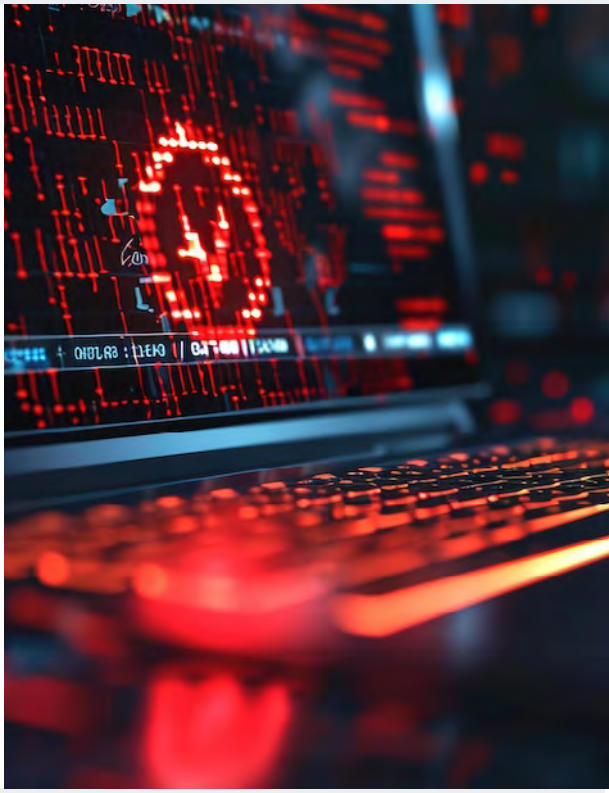


Útočníci skúšajú zneužiť kritickú zraniteľnosť v Oracle E-Business Suite týždeň po oprave

Spoločnosť Previdian zaznamenala od 22. októbra 2026 vo svojich honeypotoch pokusy o zneužitie kritickej zraniteľnosti CVE-2026-101767 (CVSS 9,8) v Oracle E-Business Suite, ktorú Oracle opravila v októbrovom Critical Patch Update. Na zraniteľnosť sú dostupné PoC exploity. Organizáciám, ktoré prevádzkujú Oracle EBS, sa odporúča bezodkladne nainštalovať Critical Patch Update z októbra 2026.

Ukradnuté prihlasovacie údaje aplikácie ConnectWise otvorili útočníkom vyše 160 tenantov Microsoft 365

Spoločnosť Huntress zdokumentovala, ako útočník 15. októbra 2026 zneužil kompromitovaný tajný kľúč aplikácie ConnectWise Cloud Backup (predtým SkyKick) a pod jej identitou získal prístupové tokeny Microsoft Graph. Spoločnosť Huntress potvrdila neoprávnené prihlásenia v 162 tenantoch Microsoft 365 poskytovateľov MSP a ich zákazníkov, pri ktorých útočník obišiel heslá aj viacfaktorovú autentifikáciu. Tokeny niesli oprávnenia aplikácie, ktoré môžu zahŕňať poštové schránky, súbory, Teams a adresárové údaje. V dvoch tenantoch si aplikácia ConnectWise pre Teams pridelila rolu Global Administrator a pridala tajné kľúče ďalším aplikáciám. ConnectWise dotknuté aplikácie deaktivovala a Microsoft aktivitu pripísala aktérovi Storm-0940. Huntress odporúča tieto aplikácie deaktivovať a preveriť roly, tajné kľúče a certifikáty podnikových aplikácií pridané od 13. októbra.





Sprostredkovateľ prístupu CyberXero s pomocou AI agentov útočil na Ukrajinu aj na poľskú štátnu správu

Spoločnosť SOCRadar odhalila operáciu rusky hovoriaceho, finančne motivovaného sprostredkovateľa počiatočného prístupu CyberXero, ktorý svoje nástroje riadi vrstvou AI agentov (až 51 agentov Claude Code). Popri automatizovanom zneužívaní platforiem WordPress a e-commerce cielene útočil na ukrajinskú energetiku a kritickú infraštruktúru a potvrdene exfiltroval dáta zo štyroch ukrajinských organizácií. V jeho držbe sú údaje o viac ako 628 000 obyvateľoch Ukrajiny. Druhou najviac zasiahnutou krajinou bolo Poľsko, kde kompromitoval e-commerce platformy a pokúšal sa zneužiť WordPress na weboch štátnej správy. Celkovo zasiahol viac ako 40 organizácií. Operáciu odhalil otvorený adresár na serveri útočníka s viac ako 90 000 súbormi.

VÝZNAMNÉ UDALOSTI VO SVETE



Ukradnuté relácie Microsoft 365 viedli ku kompromitácii 97 účtov v 79 organizáciách

Výskumníci spoločnosti Huntress opísali kampaň, v ktorej útočníci od 14. júla do 22. septembra 2026 hromadne opakovane používali ukradnuté prístupové tokeny Microsoft 365 (technika „token spraying“). Tokeny získavali okrem iného cez AitM proxy za falošnými prihlasovacími stránkami a phishingom zneužívajúcim prihlasovanie kódom zariadenia. Z viac ako 200 000 pokusov bolo 497 úspešných prihlásení. Kompromitovaných bolo 97 účtov v 79 organizáciách. Útočníci registrovali najmenej 48 falošných zariadení v Entra ID, pridávali vlastné autentifikačné aplikácie, v najmenej 19 organizáciách odstránili pôvodné metódy MFA a vytvárali skryté pravidlá schránok pre e-maily o mzdách. Huntress odporúča zneplatniť relácie, preveriť zariadenia a metódy MFA v Entra ID a obmedziť prihlasovanie kódom zariadenia pomocou Conditional Access.

Útočníci zneužívajú kritickú zraniteľnosť v module Bricksforge pre WordPress

Spoločnosť Patchstack zaznamenala aktívne zneužívanie kritickej zraniteľnosti CVE-2026-85097 (CVSS 10,0) vo WordPress plugine Bricksforge vo verziách do 3.1.8.9 vrátane. Nedostatočná kontrola nahrávaných súborov umožňuje útočníkovi bez prihlásenia nahrať a spustiť ľubovoľný PHP kód a získať kontrolu nad webom. Útoky prišli zo 63 IP adries a cielia na koncové body pre odosielanie formulárov, pričom obchádzajú filtre pomocou alternatívnych či zakódovaných prípon PHP. Oprava je vo verzii 3.1.8.10, odporúča sa aktualizovať na najnovšiu verziu 4.0.1.





Falošné desktopové aplikácie ChatGPT a Claude na GitHube šíria malvér

Spoločnosť Check Point Research odhalila kampaň Yoba, v ktorej útočníci cez falošné projekty na GitHube ponúkajú údajné desktopové verzie ChatGPT a Claude. Archívy obsahujú legitímny podpísaný spustiteľný súbor od OpenAI alebo Anthropic a vedľa neho škodlivú knižnicu, ktorú program načíta technikou DLL sideloading. Malvér YobaDropper a YobaLoader získava ďalšiu fázu cez kanál na Telegrame a DNS-over-HTTPS a nakoniec do procesu svchost.exe vloží nástroj na ťažbu kryptomien XMRig. Výskumníci predpokladajú, že útočníci na zvýšenie viditeľnosti projektov vo vyhľadávači využívajú techniku SEO poisoning.

VÝZNAMNÉ UDALOSTI VO SVETE



Binance prišla pri útoku o aktíva za 6,3 miliardy USD, stopa vedie do KĽDR

Kryptomenová burza Binance oznámila bezpečnostný incident, pri ktorom boli zasiahnuté aktíva v hodnote približne 6,3 miliardy USD. Takmer 3 miliardy USD sa podarilo zmraziť. Predbežné vyšetrovanie naznačuje kompromitáciu notebooku pracovníka DevOps a následné neoprávnené výbery. Burza dočasne pozastavila vklady a výbery a deklarovala pokrytie strát klientov. Spoločnosť TRM Labs pripisuje útok s vysokou mierou istoty severokórejskej skupine TraderTraitor.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Aktívne zneužívané kritické zraniteľnosti Citrix Netscaler

Citrix upozornil na dve kritické zraniteľnosti v NetScaler ADC a NetScaler Gateway, ktoré umožňujú neautentifikovanému útočníkovi na diaľku spustiť ľubovoľný kód. Citrix potvrdil ich aktívne zneužívanie. Opravil aj ďalšiu aktívne zneužívanú zraniteľnosť s vysokou závažnosťou, ktorou môže vzdialený útočník spôsobiť nedostupnosť služby (DoS).

Zraniteľnosť produktov Atlassian aktívne zneužívaná

Spoločnosť Atlassian opravila aktívne zneužívanú kritickú zraniteľnosť v produktoch Jira Software, Jira Service Management Data Center, Confluence Data Center, Bitbucket Data Center, Bamboo Data Center, Crowd Data Center, Crucible a Fisheye. Zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi čítať ľubovoľné súbory v koreňovom adresári aplikácie, pokiaľ pozná ich názov a súborovú cestu.

Kritické zraniteľnosti Cisco License On-Prem (SSM On-Prem)

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre Cisco License On-Prem (predtým Smart Software Manager On-Prem), ktoré opravujú interne objavené tri kritické a jednu vysoko závažnú zraniteľnosť. Zraniteľnosti umožňujú vzdialene injektovať kód, pristupovať bez autentifikácie ku kritickým funkciám, či citlivým informáciám.

Cisco opravila kritické zraniteľnosti v APIC

Spoločnosť Cisco vydala bezpečnostné aktualizácie pre Cisco Application Policy Infrastructure Controller (APIC), ktoré opravujú interne objavené kritické zraniteľnosti. Tri kritické zraniteľnosti súvisia s chybami v narábaní s rôznymi zdrojmi v rámci ich životného cyklu, nevhodným spôsobom neutralizácie nebezpečných prvkov a nesprávnym riadením prístupov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Cisco Secure Email Gateway má aktívne zneužívanú kritickú zraniteľnosť

Spoločnosť Cisco opravila kritickú aktívne zneužívanú zraniteľnosť vo funkcii Advanced Malware Protection produktu Cisco Secure Email Gateway, ktorá neautentifikovanému vzdialenému útočníkovi umožňuje prostredníctvom e-mailu so špeciálne upravenou prílohou zapisovať ľubovoľné súbory a vykonávať príkazy s oprávneniami používateľa root.

Zraniteľnosť vo FortiMail umožňuje zapisovať ľubovoľné súbory

Fortinet opravil vo FortiMail kritickú zraniteľnosť CVE-2026-104286 (prechod adresármi), ktorá umožňuje neautentifikovanému vzdialenému útočníkovi zapisovať súbory do systému cez upravené HTTP/HTTPS požiadavky. To môže viesť k spusteniu kódu a úplnej kompromitácii zariadenia. Zraniteľnosť je aktívne zneužívaná a v katalógu CISA KEV je od 1. októbra 2026. Odporúča sa bezodkladne aktualizovať.

Kritická zraniteľnosť Splunk Enterprise umožňuje vykonávať príkazy OS

Vývojári spoločnosti Splunk opravili kritickú zraniteľnosť v produkte Splunk Enterprise, pri ktorej chýbajúca autentifikácia v rozhraní Patroni REST API umožňuje neautentifikovanému útočníkovi so sieťovým prístupom k členovi clustra „search head“ vykonať ľubovoľné príkazy OS.

Kritické zraniteľnosti NGINX umožňujú spôsobiť nedostupnosť služby

Spoločnosť F5 opravila 3 kritické zraniteľnosti v NGINX Plus a NGINX Open Source, ktorých zneužitím môže vzdialený neautentifikovaný útočník prostredníctvom špeciálne upravených HTTP požiadaviek spôsobiť nedostupnosť služby (DoS) a pri vypnutej ochrane ASLR alebo jej úspešnom obídení môže získať schopnosť vykonávať kód.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti MariaDB

Vývojári databázového servera MariaDB opravili tri kritické zraniteľnosti, ktoré súvisia s chybami jeho komponentov pri narábaní s pamäťou a s obchádzaním moderného kódovania názvov tabuliek a súborov. Vzdialenému útočníkovi s nízkymi oprávneniami umožňujú vykonávať kód, spôsobiť nedostupnosť služby a získavať či meniť dáta.

Oracle opravila 1295 zraniteľností

Spoločnosť Oracle vydala októbrovú aktualizáciu Critical Patch Update, ktorá obsahuje 1 295 bezpečnostných záplat v 129 produktoch, vrátane opráv 89 kritických zraniteľností. Šesť z nich dosiahlo maximálne skóre CVSS 10,0. Mnohé kritické zraniteľnosti môže útočník zneužiť na diaľku, bez potreby autentifikácie.

PHP má dve kritické zero-day zraniteľnosti

Vývojári jazyka PHP vydali opravy dvoch kritických zraniteľností, ktoré umožňujú neautentifikované vzdialené vykonávanie ľubovoľného kódu na zraniteľnom serveri. Stručná informácia o zraniteľnostiach unikla na verejnosť pred vydaním opravných aktualizácií.

V Node.js opravili desať zraniteľností

Vývojári Node.js vydali bezpečnostné aktualizácie opravujúce desať zraniteľností, z ktorých najzávažnejšia sa nachádza v dekodéri kompresnej knižnice Brotli. Kritická zraniteľnosť umožňuje neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorených komprimovaných údajov vyvolať poškodenie pamäte, znefunkčniť službu, získať prístup ku citlivým informáciám alebo potenciálne vzdialene vykonávať kód.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zero-day zraniteľnosti jadra Linuxu

Na verejných mailing listoch pre Linux kernel boli zverejnené technické informácie viacerých ešte neopravených zraniteľností linuxového jadra. Ku šiestim z nich boli zverejnené stručné informácie. Útočníkom umožňujú vzdialene vykonávať kód, lokálne eskalovať svoje oprávnenia a získať prístup k citlivých informáciám. Najzávažnejšie zraniteľnosti sa nachádzajú v implementácii protokolu SMB.

Kritická zraniteľnosť TCP v jadre Linux umožňuje vykonávať príkazy

Vývojári jadra operačného systému Linux opravili kritickú zraniteľnosť, ktorá dovoľuje vzdialenému neautentifikovanému útočníkovi vykonávať na zraniteľnom serveri príkazy s oprávneniami používateľa root.

Zraniteľnosť DNS resolvera BIND vedie k nedostupnosti služby

Vývojári BIND, softvéru pre implementáciu protokolu DNS, opravili vysoko závažnú zraniteľnosť, ktorá umožňuje vzdialenému neautorizovanému útočníkovi spôsobiť vyčerpanie zdrojov servera a jeho nedostupnosť.

Kritická zraniteľnosť FortiSandbox

Spoločnosť Fortinet opravila kritickú zraniteľnosť v nástroji FortiSandbox, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi obísť prihlásenie do grafickej konzoly.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti Wasmtime vedú k úniku zo sandboxu

Vývojári runtime prostredia Wasmtime opravili dve kritické zraniteľnosti v kompilátore Cranelift, ktoré umožňujú vzdialenému útočníkovi s kontrolou nad kódom, ktorý vstupuje do procesu, spôsobiť nežiaduce správanie kódu a uniknúť zo sandboxu Wasm.

Vo Veeam Backup & Replication opravili štyri zraniteľnosti

Vývojári zálohovacieho nástroja Veeam Backup & Replication vydali opravy štyroch zraniteľností. Jedna je hodnotená ako kritická, jedna vysoko závažná a dve stredne závažné. Útočníkom umožňujú obísť autorizáciu, získať vysoké oprávnenia a zapisovať súbory na ľubovoľné miesto na zálohovacom serveri.

MESAČNÍK ZRANITEĽNOSTÍ OKTÓBER 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/4199.html