Postřehy z bezpečnosti: nový typ DoS útoku na protokoly využívající UDP

root.cz/clanky/postrehy-z-bezpecnosti-novy-typ-dos-utoku-na-protokoly-vyuzivajici-udp/

Autor: Root.cz s využitím DALL-E

V dnešním díle Postřehů se podíváme na nový typ DoS útoku na UDP protokoly, zranitelnosti umožňující otevírat miliony dveří v hotelech po celém světě nebo pokračující problémy s databází NVD.

DoS útok na protokoly využívající UDP

Výzkumný tým z německého institutu CISPA Helmholtz Center for Information Security publikoval v úterý informaci o novém typu DoS útoku, který byl nazván „Loop DoS“ a který je možné provést proti vybraným implementacím aplikačních protokolů využívajících pro přenos dat transportní protokol UDP.

Útok je principiálně založený na spuštění vzájemné komunikace dvou „zranitelných“ síťových služeb, které si následně v nekonečné smyčce začnou vyměňovat informace, v důsledku čehož vzniknou datové toky, které mohou mít dopad na dostupnost komunikujících systémů a/nebo jimi využívané síťové infrastruktury.

Útokem jsou zranitelné služby, které odpovídají chybovou hláškou v případě, kdy je jim rovněž zaslána chybová hláška. Pokud se tímto způsobem chovají např. dva servery DNS či NTP, útočníkovi postačuje podvrhnout zdrojovou IP adresu prvního z nich v „iniciační“ zprávě s chybovým vstupem zaslané druhému serveru, a zajistí tím, že oba zranitelné servery si budou následně donekonečna vyměňovat zprávy obsahující chybové hlášky.

Dle odhadů výzkumného týmu je možné útok úspěšně realizovat proti přibližně 300 000 systémům různých výrobců (mj. Microsoft nebo MikroTik) aktuálně dostupným z internetu.

Zranitelnosti elektronických zámků

Skupina nezávislých bezpečnostních výzkumníků publikovala v uplynulém týdnu informaci o existenci série zranitelností, které postihují elektronické RFID zámky Saflok společnosti dormakaba, užívané zejména v prostředí hotelů. Zranitelnosti, dohromady nazvané Unsaflok, údajně umožňují otevřít libovolné dveře v objektu, v němž jsou zranitelné zámky instalovány, s pomocí jediného páru „padělaných“ vstupních karet.

Zranitelné zámky byly dle publikovaných informací instalovány ve více než 3 milionech dveří ve více než 13 000 lokalitách ve 131 zemích světa, včetně České republiky.

Zranitelnosti byly výzkumným týmem identifikovány a nahlášeny již v září 2022 a záplaty pro ně byly publikovány v listopadu 2023, nicméně do současnosti bylo dle odhadů výzkumného týmu záplatováno nebo nahrazeno jen okolo 36 % všech zranitelných zámků.

Detailní informace o postupu pro zneužití zranitelností prozatím publikovány nebyly, nicméně výzkumný tým ve svém prohlášení uvedl, že úspěšný útok je možné provést při získání libovolné validní (i expirované) vstupní karty z cílového objektu s pomocí páru MIFARE Classic karet, nebo s pomocí libovolné platformy, která tento formát umožňuje emulovat (např. Flipper Zero).

Pokračující problémy s National Vulnerability Database

National Vulnerability Database (NVD) je – jak již název napovídá – databází s informacemi o zranitelnostech postihujících SW produkty. Nejde však o databázi ledajakou, ale o primární zdroj detailních informací ke všem zranitelnostem, kterým kdy byly přiřazeny CVE identifikátory, neb k těmto zranitelnostem poskytuje dodatečný kontext (popisy, CVSS skóre, mapování na CPE, odkazy relevantní na externí materiály apod.) na základě analýz specialistů z amerického federálního standardizačního úřadu NIST, který databázi provozuje.

Přestože nejde o jedinou velkou databázi, v níž jsou informace o zranitelnostech obsaženy, je NVD unikátním a vysoce významným vstupem pro jakékoli systémy nebo procesy zaměřené na řízení zranitelností. Zdá se však, že nad pokračujícím fungováním NVD visí otazníky. 15. února se totiž na jejích oficiálních stránkách objevila informace o tom, že „NIST v současné době pracuje na vytvoření konsorcia, které by řešilo výzvy spojené s programem NVD“ a v souvislosti s tím dojde k „dočasným prodlevám“ v aktivitách spojených s analýzami zranitelností.

Jak dlouhé ony „dočasné prodlevy“ budou do současnosti není jasné. Již od 12. února však začal NIST publikovat v NVD velké množství záznamů, které nebyly z jeho strany analyzovány, a za měsíc od publikace výše zmíněné zprávy byl ze strany analytiků NISTu

doplněn kontext v podobě metadat pouze k cca 10 % zranitelností nově přidaných do NVD.

V souvislosti s touto skutečností se v uplynulém týdnu v rámci odborné komunity i odborných médií objevila řada hlasů volajících po brzkém plném obnovení funkce NVD, i po otevření diskuze o nahrazení této databáze nějakým jiným (a potenciálně spolehlivějším) datovým zdrojem.

NIST sám se v době přípravy tohoto textu k aktuálním problémům ani dalšímu očekávanému vývoji oficiálně nevyjádřil.

Soutěž PWN2OWN přinesla řadu nových zranitelností

V uplynulém týdnu proběhl první letošní běh soutěže PWN2OWN organizované ze strany Zero Day Initiative a zaměřené na demonstraci nových zranitelností a 0-day útoků.

Vedle úspěšného útoku na řídící jednotku automobilů Tesla, za jehož demonstraci byli výzkumníci odměněni jak vozem stejné značky, tak významným finančním obnosem, byly demonstrovány například i VM escape zranitelnosti pro VMware Workstation a Oracle VirtualBox, nebo exploity pro Chrome, Safari či Firefox.

Celkem účastníci soutěže demonstrovali 29 unikátních exploitů, za které si odnesli finanční odměny přesahující v celkové výši 1,1 milionu dolarů.

Detailní výsledky prvního a druhého dne soutěže jsou k dispozici na webu ZDI.

Ruské útoky nejen na Ukrajinu

Společnost SentinelLabs ve čtvrtek zveřejnila analýzu nedávného kybernetického útoku na ukrajinské poskytovatele internetového připojení, v důsledku něhož museli postižení ISP dočasně omezit poskytování svých služeb.

Při útoku byl využit wiper nazvaný AcidPour – modifikovaná verze nástroje AcidRain, který byl použit při útoku na satelitní modemy v den začátku války na Ukrajině. K útoku se přihlásila skupina Solntsepek, která má údajné vazby na ruskou vojenskou zpravodajskou službu GRU.

Malware AcidPour však nebyl jediným faktorem z poslední doby, který měl dopad na poskytovatele internetového připojení na Ukrajině.

Masivní ruský útok na ukrajinské energetické systémy z konce uplynulého týdne, při němž bylo využito celkem 150 raket a dronů, totiž způsobil vedle významných fyzických škod a ztrát na životech také citelné omezení dostupnosti internetu ve vybraných částech země.

Zmínku zaslouží, že tomuto útoku předcházela mj. i dezinformační kampaň vedená s pomocí mediálních a telegramových kanálů, v rámci níž se Rusové pokusili způsobit paniku v souvislosti se smyšleným hrozícím protržením hráze Dněperské vodní

elektrárny. Ruská strana dezinformační a vlivové operace dlouhodobě využívá nejen při cílení na Ukrajinu.

Právě v souvislosti s participací na podobných operacích uvalilo v uplynulém týdnu ministerstvo financí USA sankce na dva ruské občany a dvě ruské organizace, které se měly podílet na dezinformačních kampaních, při nichž mělo být využito přes 60 falešných vládních a mediálních webových portálů k šíření nepravdivých informací.

Pro úplnost je v souvislosti s ruskými aktivitami vhodné zmínit rovněž, že analytici společnosti Mandiant v pátek publikovali zprávu věnovanou analýze útoků na německé politiky, při nichž byly využity phishingové zprávy distribuující backdoor nazvaný WINELOADER, přičemž tuto útočnou kampaň analytici jednoznačně připsali ruské skupině APT-29.

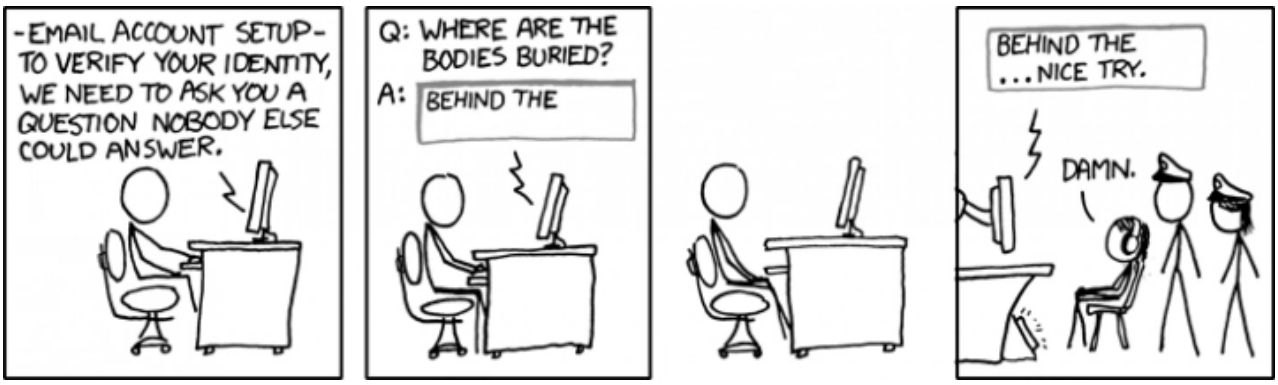
V kontextu kybernetických útoků a Ruska zaslouží zmínku též, že telekomunikační regulátor Roskomnadzor koncem předminulého týdne informoval, že v souvislosti s nedávnými prezidentskými volbami evidovala tato agentura významné množství DDoS útoků na ruské systémy související s volbami, nicméně dopad těchto útoků na vlastní volební proces byl údajně nulový.

Další zajímavosti

- NÚKIB zřejmě nestihne termín transpozice směrnice NIS2
- Vojenské zpravodajství údajně poprvé aktivně zasáhlo v kybernetickém prostoru
- Microsoft do konce měsíce plánuje omezit přístup ruských organizací k více než 50 cloudovým službám
- V chybně nakonfigurovaných Firebase instancích bylo nalezeno téměř 19 milionů hesel v čitelné podobě
- V kampani Sign1 bylo kompromitováno přes 39 000 webových portálů založených na platformě WordPress
- ENISA slaví 20 let své existence
- Publikován GoFetch – nový útok umožňující extrahovat postranním kanálem kryptografické klíče z procesorů Apple
- GitHub spustil veřejnou betu AI nástroje automaticky navrhujícího opravy zranitelností v kódu
- Americké úřady varovaly před kybernetickými útoky zaměřenými na vodovodní systémy
- Valné shromáždění OSN přijalo první globální rezoluci o AI
- Skupina Earth Krahang, která má potenciální vazby na Čínu, od roku 2022 úspěšně kompromitovala 48 vládních organizací různých států z celého světa
- Skupina s vazbami na Írán tvrdí, že úspěšně pronikla do sítě izraelského jaderného výzkumného zařízení
- Google představil novou podobu služby Safe Browsing v prohlížeči Chrome
- Škodlivé globální téma pro KDE bylo využito pro mazání dat
- Byla publikována nová kritická zranitelnost postihující Ivanti Standalone Sentry

- Microsoft publikoval záplatu pro zranitelnost Xbox Gaming Service poté, co pro nic byl zveřejněn PoC exploit
- Byli vyhlášení vítězové Big Brother Awards za rok 2023
- Microsoft publikoval out-of-band update, který opravuje nedávnou záplatu způsobující pády doménových řadičů
- Německá policie provedla úspěšný zásah proti darkwebovému tržišti Nemesis Marketplace
- Ukrajinská policie zadržela 3 členy skupiny podezřelé z prodeje milionů zcizených e-mailových a instagramových účtů
- CISA a FBI publikovaly společné doporučení pro efektivní reakci na DDoS útoky
- Panel OSN vyšetřuje 58 kybernetických útoků zaměřených na krádeže kryptoměn, za nimiž údajně stála Severní Korea
- Byly publikovány záplaty pro kritické zranitelnosti v prohlížečích Firefox a Chrome
- Microsoft oznámil konec podpory pro RSA klíče kratší než 2048 bitů v operačních systémech Windows
- Esport turnaj ve hře Apex Legends pozastaven po kompromitaci počítačů dvou soutěžících
- Kanada zřejmě přehodnotí své rozhodnutí o zákazu prodeje platformy Flipper Zero
- Používání VPN v Texasu se po zablokování přístupu k portálu PornHub z tohoto státu zvýšilo o 234 %

Pro pobavení



Let's invite him to a party and play ‚I never'. Okay, I never hid any bodies SOUTH of Main Street. … he's taking a drink!

Autor: Randall Munroe, podle licence: CC BY-NC 2.5

O seriálu

Tento seriál vychází střídavě za pomoci pracovníků Národního bezpečnostního týmu CSIRT.CZ provozovaného sdružením CZ.NIC a bezpečnostního týmu CESNET-CERTS sdružení CESNET, bezpečnostního týmu CDT-CERT provozovaného společností ČD Telematika a bezpečnostních specialistů Jana Kopřivy ze společnosti Nettles Consulting a Moniky Kutějové ze sdružení TheCyberValkyries. Více o seriálu…

Vstoupit do diskuse (11 názorů)

Autor článku

Jan Kopřiva je specialistou na kybernetickou bezpečnost s dlouhou praxí a širokými zkušenostmi. V současnosti působí jako bezpečnostní konzultant ve společnosti Nettles Consulting a také jako jeden z odborníků ve sdružení SANS Internet Storm Center.

Ja na rozdil od vas ten realny provoz resim, pane kolego. A utoky, v nichz na strane zdrojoveho i ciloveho portu je nejaky ephemeral port zas tak neobvykle nejsou.

Danny Stříbrný podporovatel