MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

December 2021

Vypracoval: CSIRT.SK

TLP: White

Sviatočná nálada a nádej na pokojné a pohodové sviatky sa rozplynula bezpečnostným tímom na celom svete po tom, ako spoločnosť LunaSec publikovala 9.12.2021 informáciu o kritickej zraniteľnosti Log4Shell (CVE-2021-44228). Chybu v logovacej knižnici Java Log4J v2 objavil dva týždne predtým Chen Zhaojun, člen Alibaba Cloud Security Team.

Log4J v2 vyvíja spoločnosť Apache Software Foundation. Popularita tejto knižnice programovacieho jazyka Java slúžiacej na manažment logovania a s ňou spojená širokoškála implementácia sú dôvodom paniky, ktorá vznikla ohľadom zraniteľnosti Log4J. Na internete sa objavili nadpisy článkov predznamenávajúce kybernetickú katastrofu globálnych rozmerov. Knižnicu Log4J využívali v decembri 2021 tisícky spoločností po celom svete. Bola implementovaná v desiatkach populárnych produktov a rádovo väčšom počte softvérových produktov vyvíjaných na mieru.

Zároveň spôsob zneužitia zraniteľnosti Log4Shell je veľmi jednoduchý. Neautentifikovaný útočník môže vzdialene poslať dostupnej zraniteľnej službe požiadavku interpretovanú v rozhraní JNDI. Systém túto požiadavku zaloguje cez komponent Log4J. Log4J tento záznam interpretuje ako príkaz, ktorý vykoná. Server môže kontaktovať adresu, ktorú zadal útočník, odkiaľ sa môže napríklad stiahnuť malvér, ktorý sa spustí. Zraniteľnosť je tak spájaná hneď s niekoľkými bezpečnostnými problémami. Knižnica nedostatočne validuje a ošetruje používateľské vstupy. Tiež umožňuje vzdialeným používateľom bez oprávnení dopytovať sa na informácie využitím sekvencie znakov ${……}. Umožnenie vykonávania príkazov v kontexte zraniteľnej aplikácie dovoľuje útočníkovi dosiahnuť únik citlivých informácií o zraniteľnom systéme, alebo vzdialené vykonávanie kódu, vďaka čomu môže útočník napríklad jednoduchým spôsobom inštalovať malvér na zraniteľný server. Možných spôsobov zneužitia Log4Shell existuje však viacero.

Zneužívanie zraniteľnosti bolo pozorované v súvislosti so šírením ransomvéru Night Sky, ktorý sa objavil začiatkom roka 2022, pravdepodobne v biznis modeli RaaS. Zneužíval ju aj ransomvér Khonsari a remote access trojany Cobalt Strike, Meterpreter a Bladabindi.

Za zmienku stojí aj samotný proces opravy zraniteľnosti knižnice. Nebol priamočiary, ako by sme očakávali, ale nabral formu Odyssei. Oprava zraniteľnosti CVE-2021-44228 uzrela svetlo sveta už 6. decembra. Vo verzii 2.15.0 však bola odhalená nová kritická zraniteľnosť umožňujúca vzdialene vykonávať kód. Preto o týždeň vývojári publikovali verziu Log4J 2.16.0. Aj táto verzia sa však v najbližších dňoch ukázala ako zraniteľná. Tentokrát bolo možné nekonečnou slučkou vo vyhľadávaní spôsobiť odmietnutie služby (DoS). 17. decembra preto spoločnosť Apache vydala opravenú verziu 2.17.0. Nočná mora vývojárov sa však zopakovala. Nová verzia obsahovala stredne závažnú zraniteľnosť umožňujúcu vzdialene vykonávať kód. 27. decembra tak uzrela svetlo sveta verzia 2.17.1, ktorá si zatiaľ udržuje svoju pozíciu. Pre staršie verzie Java je to Log4J 2.12.4 (Java 7) a 2.3.2 (Java 6).

Vzhľadom na popularitu knižnice Log4J v2 a komplikovanosť jej aktualizácie v mnohých produktoch viacerí odborníci predpokladajú, že táto hrozba s nami ostane ešte niekoľko rokov.

Preto ak ste tak ešte neurobili, odporúčame vám urobiť dôkladný audit vašej IT infraštruktúry a kontaktovať dodávateľov produktov a systémov, ktoré používate, s otázkou, či neobsahujú zraniteľné verzie Log4j. Pokiaľ zraniteľné produkty objavíte, pristúpte k sanácii a odstráneniu zraniteľností s predpokladom, že vaša infraštruktúra bola kompromitovaná.

Tím CSIRT.SK vám praje veľa úspechov v novom roku vo všetkých oblastiach vášho života. Zároveň vám srdečne želáme, aby ste nepotrebovali dosahovať úspechy pri obnove vašej infraštruktúry a sanácii škôd po kybernetickom útoku. Šťastný a bezpečný rok 2022!

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci december riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Jednotka riešila tiež prípady kompromitovaných e-mailových schránok zamestnancov niekoľkých verejných a súkromných organizácií v Slovenskej republike, odkiaľ útočníci posielali phishingové správy aj na zamestnancov inštitúcií v konštituencii jednotky. Dôveryhodnosť škodlivých e-mailov sa pokúšali podporiť ich vložením do vlákien staršej legitímnej komunikácie. Tieto kampane však boli podľa získaných informácií neúspešné.

Hlavnou udalosťou mesiaca december bolo odhalenie kritickej zraniteľnosti logovacej knižnice jazyka Java, Apache Log4j v2, ktorú využíva veľké množstvo softvérových produktov a systémov. Táto zraniteľnosť vyvolala paniku a vzbudila pozornosť bezpečnostnej komunity na celom svete. CSIRT.SK v nedeľu 12.12.2021 e-mailom rozposlal varovanie kontaktným osobám vo svojej konštituencii a vydal varovanie na svojom webe. Následne začal zber informácií o zastúpení Log4j v IT infraštruktúrach jednotlivých organizácií vo svojej pôsobnosti a dohľad nad mitigáciou ich zraniteľných systémov.
Krátko po publikovaní informácií a ukážok jej zneužitia sa o zraniteľnosť začali vo veľkej miere zaujímať útočníci a využívať ju napríklad na infikovanie zraniteľných systémov ransomvérom. V rámci konštituencie CSIRT.SK nebol však podobný incident hlásený. Vzhľadom na širokú implementáciu knižnice Log4j ostane s nami táto hrozba pravdepodobne ešte dlhú dobu.

V rámci svojej proaktívnej činnosti jednotka vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Taktiež školí zamestnancov týchto organizácií. Témy preberané v decembri súviseli so základmi informačnej bezpečnosti a s bežnými hrozbami, s ktorými sa účastníci môžu stretnúť v pracovnom aj súkromnom živote. Účastníci získali informácie, ako tieto hrozby rozpoznávať a ako sa pred nimi brániť. Prezentácia ku školeniu je dostupná na webovom sídle jednotky.

Významné útoky vo svete

Spoločnosti Planned Parenthood v Los Angeles unikli údaje o cca 400-tisíc pacientoch

Planned Parenthood Los Angeles sa medzi 9. a 17. októbrom 2021 stala obeťou útoku ransomvéru. Neoprávnená osoba získala prístup do siete spoločnosti, pričom útočník exfiltroval niektoré súbory zo systémov. Unikli údaje o približne 400-tisíc pacientoch, ktoré zahŕňali osobné údaje ako adresa, informácie o poistení, dátum narodenia a klinické informácie ako sú diagnóza a informácie o predpisoch. Nie je známe, ktorá skupina útočníkov je zodpovedná za predmetný útok. Zverejnenie údajov by mohlo výrazne ovplyvniť dotknutých pacientov, pretože útočníci vďaka údajom môžu vykonávať cielenejšie útoky.

Trójsky kôň RedLine kradne citlivé údaje z infikovaných zariadení

Útočníci spamujú kontaktné formuláre webových stránok a diskusné fóra s cieľom distribuovať súbory Excel XLL, ktoré stiahnu a nainštalujú malvér RedLine. RedLine je trójsky kôň, ktorý je schopný vykonávať príkazy, sťahovať a spúšťať ďalší malvér a vytvárať snímky obrazovky. V infikovaných zariadeniach sa zameriava na súbory cookies, používateľské mená a heslá, kreditné karty uložené vo webových prehliadačoch a ďalšie citlivé údaje. BleepingComputer zistil, že sa jedná o kampaň, ktorá sa zameriava na mnohé webové stránky využívajúce verejné fóra alebo systémy umožňujúce komentovať články.

Malvér NginRAT sa maskuje za legitímny proces nginx

Nový malvér sa na serveroch elektronických obchodov maskuje za legitímny proces. Malvér, ktorý bol pomenovaný NginRAT, sa zameriava na nginx a možnosti vzdialeného prístupu, ktoré poskytuje. Cieľom útokov je odcudzenie údajov o platobných kartách z internetových obchodov. Malvér infikoval servery v USA, Nemecku a

Francúzsku, pričom servery predtým boli infikované malvérom CronRAT. Malvéry RAT umožňujú modifikáciu kódu na strane servera. Zdá sa, že tieto 2 RAT malvéry majú rovnakú úlohu a fungujú ako záloha na zachovanie vzdialeného prístupu. Útočníci ich využívajú práve na modifikáciu kódu na strane servera, aby boli schopní zachytávať POST požiadavky zasielané používateľmi.

Výskumníci identifikovali novú skupinu útočníkov Karakurt, ktorá sa zameriava na krádež údajov a vydieranie

Nová skupina útočníkov s názvom Karakurt sa zameriava na krádež údajov a vydieranie. Útočníci nevyužívajú ransomvér na šifrovanie súborov svojich obetí. Jedná sa o skupinu, ktorej prvé známky aktivity boli identifikované v júni 2021. Výskumníkom spoločnosti Accenture Security sa podarilo vysledovať taktiky skupiny, sadu nástrojov a techniky prieniku. Skupina tvrdí, že medzi septembrom a novembrom 2021 kompromitovali viac ako 40 obetí, pričom zhruba 95% sídli v Severnej Amerike. Útočníci primárne využívajú na získanie počiatočného prístupu do siete prihlasovacie údaje do VPN a na perzistenciu využívajú Cobalt Strike alebo AnyDesk.

Útočníci ukradli spoločnosti Volvo Cars informácie o výskume a vývoji

Spoločnosť Volvo Cars zistila, že k jednému z jej súborových úložísk pristupovala neoprávnená tretia strana. Útočníci ukradli obmedzené množstvo informácií o výskume a vývoji, čo môže mať vplyv na fungovanie spoločnosti. Zákazníci a ich osobné údaje neboli ohrozené. Skupina stojaca za útokom sa nazýva Snatch, pričom 30. novembra 2021 pridala na svoju stránku ako dôkaz, že ukradla údaje, snímky ukradnutých súborov. Spoločnosť Volvo sa nevyjadrila k tomu, či snímky zverejnené ako dôkaz obsahujú naozaj súbory ukradnuté z jej serverov.

Malvér DarkWatchman v kombinácii so C# keyloggerom infikuje zariadenia

Na scéne sa objavil nový RAT malvér s názvom DarkWatchman v kombinácii so C# keyloggerom. Prvé známky aktivity tohto malvéru sa objavili v novembri 2021, kedy útočníci šírili malvér prostredníctvom phishingových emailov so škodlivými zip prílohami. Zip súbor obsahuje spustiteľný súbor používajúci ikonu textového dokumentu, ktorý nainštaluje na zariadenie RAT (Remote Access Trojan) a keylogger. DarkWatchman je malvér, ktorý využíva veľkú množinu binárnych súborov, skriptov a knižníc a zahŕňa tajné metódy na prenos údajov medzi modulmi. Je schopný spúšťať súbory .exe, načítať DLL knižnice, vykonávať príkazy, nahrať súbory na riadiaci server zo stroja obete a ďalšie rôzne činnosti.

Inštalačné programy KMSpico infikujú zariadenia s operačným systémom Windows

Výskumníci zo spoločnosti Red Canary zistili, že útočníci distribuujú upravené inštalačné programy KMSpico, aby infikovali zariadenia s operačným systémom Windows. Malvér je schopný kradnúť kryptomenové peňaženky. KMSPico je nelegitímny aktivátor produktov Microsoft Windows a Office, ktorý emuluje server Windows Key Management Services (KMS). Škodlivý inštalačný program KMSPico, ktorý analyzovala spoločnosť Red Canary, sa dodáva prostredníctvom samorozbaľovacieho spustiteľného súboru ako je 7-Zip a obsahuje skutočný emulátor servera KMS, ale aj Cryptbot. Cryptbot zhromažďuje citlivé údaje z aplikácií ako napríklad kryptomenová peňaženka Coinomi, kryptomenová peňaženka Ledger Live a iných.

Botnet Moobot sa šíri webovým serverom mnohých produktov spoločnosti Hikvision

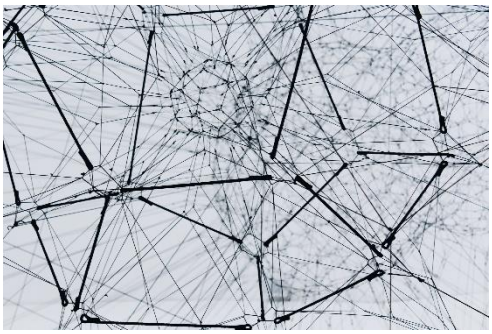
Botnet založený na Mirai s názvom Moobot sa šíri zneužívaním kritickej zraniteľnosti CVE-2021-36260 na webovom serveri mnohých produktov spoločnosti Hikvision, ktorá je čínskym výrobcom kamier a zariadení. Spomínaná zraniteľnosť súvisí s injektovaním

príkazov na predmetných serveroch. Chyba bola spoločnosťou opravená už v septembri roku 2021, avšak nie všetci používatelia stihli aplikovať bezpečnostné aktualizácie. Moobot využívajú útočníci na kompromitáciu neopravených zariadení a následné získavanie citlivých údajov. Spoločným znakom pre botnety Mirai a Moobot je napríklad dátový reťazec, ktorý sa používa vo funkcii generátora náhodných alfanumerických reťazcov.

16-tisíc rôznych IP adries útočilo na 1,6 milióna Wordpress webových stránok

Až 1,6 milióna WordPress webových stránok bolo zasiahnutých útokmi zo 16-tisíc rôznych IP adries. Útočníci sa zameriavajú na 4 doplnky a 15 tém rámca Epsilon. Medzi ovplyvnené doplnky patria PublishPress Capabilities, Kiwi Social Plugin, Pinterest Automatic a WordPress Automatic. Ovplyvnené sú témy ako napríklad Shapely, NewsMag, Activello, Illdy, Allegiant a ďalšie. Vo väčšine prípadov útočníci povolia možnosť users_can_register a možnosť default_role nastavia na administrátora, čo umožňuje útočníkom registrovať sa ako správca a prebrať tak kontrolu nad webovou stránkou.

Botnet Phorpiex distribuuje nový variant malvéru s názvom Twizt



Botnet Phorpiex, ktorý bol v minulosti vypnutý, sa objavil s novými príkazmi a riadením typu peer-to-peer. Botnet je známy od roku 2016. Po piatich rokoch sa operátori tohto botnetu rozhodli skúsiť predať zdrojový kód na hackerskom fóre. Avšak výskumníci zo spoločnosti Check Point zistili, že infraštruktúru opäť zapli v septembri roku 2021. Botnet začal distribuovať nový variant malvéru s názvom Twizt, ktorý mu umožňuje fungovať bez centralizovaných riadiacich serverov. Twizt tiež umožňuje rôznym infikovaným zariadeniam prenášať príkazy medzi sebou.

Nový spyware PseudoManuscrypt sa nápadne podobá na Manuscrypt používaný skupinou Lazarus

Bezpečnostní výskumníci spozorovali nový spyware PseudoManuscrypt, ktorý sa zameriava na vládne organizácie a priemyselné riadiace systémy v strojárstve, energetike a ďalších odvetviach. Tento spyware sa podobá malvéru Manuscrypt, ktorý bol v rámci útokov používaný skupinou Lazarus. Manuscrypt (NukeSped) je rodina malvérových nástrojov používaných na špionáž. Útočníci stojaci za malvérom PseudoManuscrypt používajú falošné archívy inštalačných súborov pirátskeho softvéru na prvotné stiahnutie spywaru do systémov. PseudoManuscrypt je schopný kradnúť prihlasovacie údaje do VPN, zaznamenávať stlačené klávesy, odpočúvať a nahrávať zvuk a iné činnosti.

- **Falošná aplikácia pre Android kradne online prihlasovacie údaje do malajzijských bánk.**
- **Emotet sa šíri prostredníctvom falošného Adobe inštalátora.**
- **Používatelia Androidu v Iráne sa stali obeťou smishingovej (SMS phishing) kampane.**
- **AT&T stále bojuje s malvérom EwDoor na VoIP serveroch.**
- **Útočníci vo phishingových kampaniach využívajú omikron variant COVID-19.**
- **Falošná podpora vyvoláva obetiam, aby si nainštalovali na svojich Android zariadeniach bankový malvér BRATA.**
- **Spoločnosť Apple varovala zamestnancov amerického ministerstva zahraničných vecí, že ich mobilné telefóny (iPhone) boli napadnuté pomocou exploitu s názvom ForcedEntry na nasadenie spywaru Pegasus.**
- **FBI varuje pred útokmi ransomvéru Cuba.**

TLP: White

- **Francúzska národná agentúra pre kybernetickú bezpečnosť ANSSI varuje pred útokmi ruskej skupiny Nobelium zameriavajúcej sa na francúzske organizácie.**
- **Hotelová spoločnosť Nordic Choice Hotels sa stala obeťou útoku ransomvéru Conti.**
- **Útočníci stojaci za útokmi na SolarWinds využívajú vo svojich útokoch nové taktiky.**
- **Spoločnosti Google sa podarilo narušiť botnet Glupteba.**
- **Nový ransomvér Cerber sa zameriava na servery Confluence a Gitlab zneužívaním RCE zraniteľností.**
- **Austrálsky poskytovateľ elektriny CS Energy sa stal obeťou útoku ransomvéru Conti.**
- **Útočníci stojaci za útokom na spoločnosť Vestas Wind Systems zverejnili ukradnuté údaje.**
- **Spoločnosť Cox Communications sa stala obeťou úniku údajov, po tom čo sa útočník vydával za podporu, aby tak získal prístup k údajom.**
- **Spoločnosť Frontier Software sa stala v novembri roku 2021 obeťou útoku ransomvéru.**
- **Malvér Anubis sa zameral na viac ako 400 finančných inštitúcií.**
- **Severoamerický distribútor propánu Superior Plus sa stal obeťou útoku ransomvéru.**
- **Ransomvér Conti zasiahol portlandský pivovar a hotelový reťazec McMenamins.**
- **Viac ako 500-tisíc používateľov Androidu si stiahlo do svojho zariadenia malvér Joker.**
- **Francúzska spoločnosť Inetum Group bola zasiahnutá ransomvérom. Zdá sa, že sa mohlo jednať o ransomvér BlackCat.**
- **Webová stránka Pro Wrestling Tees sa stala obeťou úniku údajov.**

Závažné zraniteľnosti bežných softvérových produktov

Spoločnosť HP opravila zraniteľnosti ovplyvňujúce minimálne 150 modelov multifunkčných tlačiarní

Zraniteľnosti sa v asi 150 modeloch multifunkčných zariadení spoločnosti HP (Hewlett Packard) vyskytujú už od roku 2013. Nahlásené a opravené však boli až v roku 2021. Útočníci ich môžu zneužiť na krádež informácií alebo vzdialené vykonanie kódu. Na opravu týchto chýb je nutné aktualizovať firmvér.

Závažné zraniteľnosti produktov spoločnosti Mozilla umožňujú prevziať kontrolu nad zraniteľným zariadením

Spoločnosť Mozilla opravila sériu závažných a stredne závažných chýb prítomných v jej produktoch Firefox, Firefox ESR a Thunderbird. Najzávažnejšia z nich umožňuje vykonávať ľubovoľný kód a prevziať kontrolu nad zraniteľným zariadením.

Závažná zraniteľnosť platformy WordPress umožňuje útoky cez distribučný kanál pluginov a tém

Obľúbená platforma na tvorbu webových stránok obsahuje závažnú zraniteľnosť, ktorá útočníkom umožňuje jednoduchým spôsobom vymeniť tému či plugin webstránky za jeho škodlivú verziu. To môže viesť ku vzdialenému vykonávaniu kódu a kompromitácii webstránky. Ak stránka používa vlastný neregistrovaný doplnok, útočníkovi stačí zaregistrovať svoj plugin na webe wordpress.org s rovnakým názvom. V rámci automatickej aktualizácie si následne stránka stiahne škodlivú verziu.

Zraniteľnosť CVE-2021-44228 (Log4Shell)

Dňa 9.12.2021 bola zverejnená informácia o zraniteľnosti knižnice Log4j vo verzii 2 od spoločnosti The Apache Software Foundation. Zraniteľnosť s označením CVE-2021-44228 (Log4Shell, LogJam) a vysokou závažnosťou umožňuje vzdialené spustenie kódu.

V zariadeniach SMA spoločnosti SonicWall sa vyskytuje 8 zraniteľností

Spoločnosť SonicWall opravila 8 zraniteľností v zariadeniach Secure Mobile Access (SMA) série 100, z čoho 2 sú kritické, 4 závažné a 2 stredne závažné. Dôsledkom zneužitia týchto zraniteľností môže byť vzdialené vykonanie kódu na zraniteľnom zariadení.

Mesačník zraniteľností December 2021

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné závažné zraniteľnosti
    - Spoločnosť HP opravila zraniteľnosti ovplyvňujúce minimálne 150 modelov multifunkčných tlačiarní
    - Závažné zraniteľnosti produktov spoločnosti Mozilla umožňujú prevziať kontrolu nad zraniteľným zariadením
    - Závažná zraniteľnosť platformy WordPress umožňuje útoky cez distribučný kanál pluginov a tém
    - Zraniteľnosť CVE-2021-44228 (Log4Shell)
    - V zariadeniach SMA spoločnosti SonicWall sa vyskytuje 8 zraniteľností

https://www.csirt.gov.sk/posts/2688.html?csrt=16864577055945964709