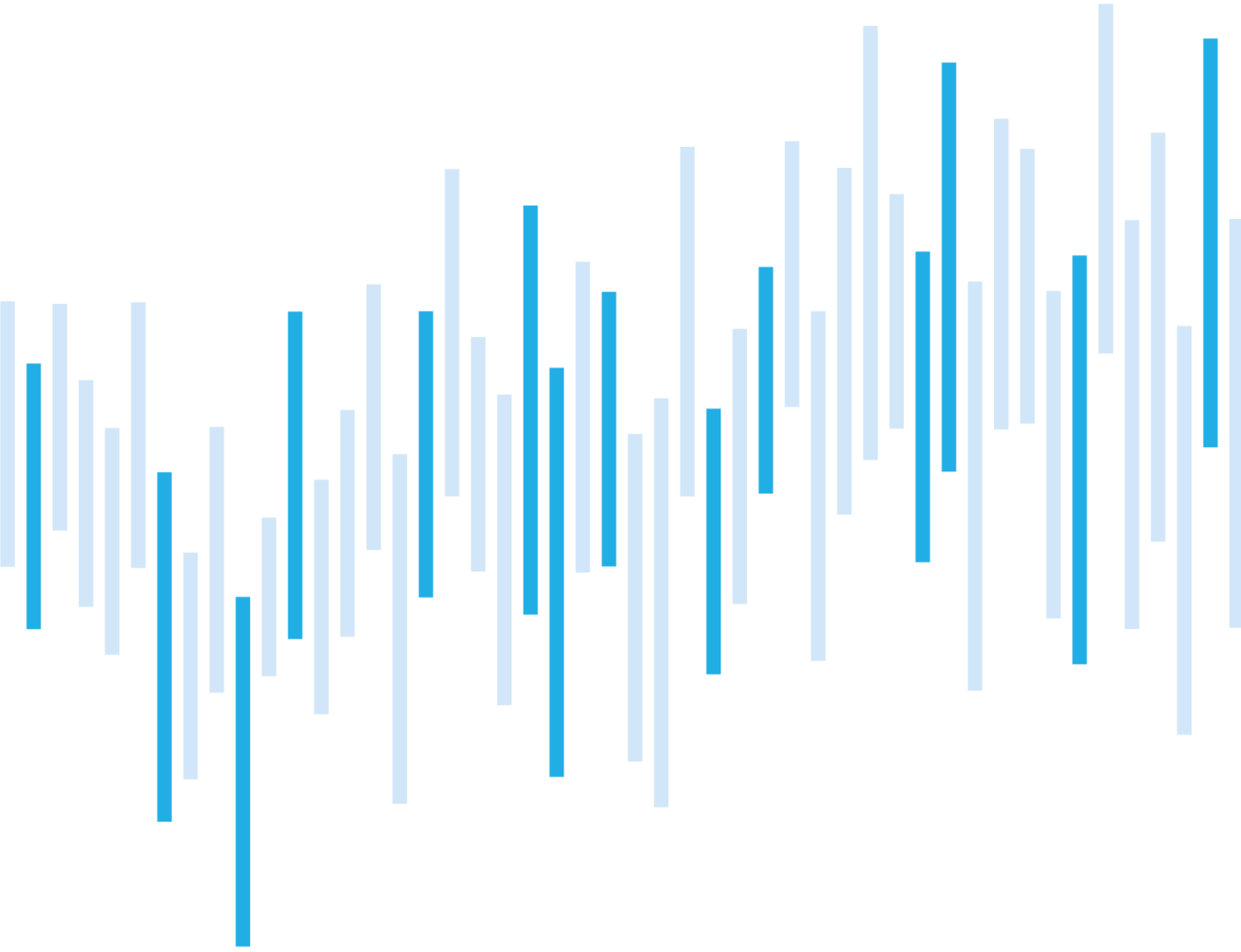
Kybernetické incidenty pohledem NÚKIB

PROSINEC 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V prosinci otřáslo světovou i českou kybernetickou scénou zveřejnění zranitelnosti CVE-2021-44228, která je také známá jako Log4Shell. Log4Shell je velmi závažná zranitelnost, která potenciálně postihuje stovky miliónů systémů. Kód pro její zneužití je volně dostupný a útočník nemusí mít velké technické schopnosti, aby ho zvládl použít. Útočníci díky němu mohou získat přístupové údaje svých obětí, exfiltrovat data či instalovat další škodlivé kódy, včetně ransomwarů.

Navzdory obavám se zneužívání zranitelnosti do prosincových kybernetických incidentů výrazněji nepromítlo. Pouze dva z 15 incidentů, které NÚKIB řešil, byly spojené s Log4Shell. Je ale pravděpodobné (55–70 %), že zneužívání Log4Shell je teprve na začátku a v dalších měsících budou incidenty přibývat. APT skupiny si postupně přidávají kód pro zneužití Log4Shell do svých toolboxů a ransomwarové skupiny kupují přístupy do systémů, které jsou vůči Log4Shell zranitelné. Je tak pravděpodobné (55–70 %), že Log4Shell v následujících měsících otevře dveře do mnoha organizací, včetně těch českých.

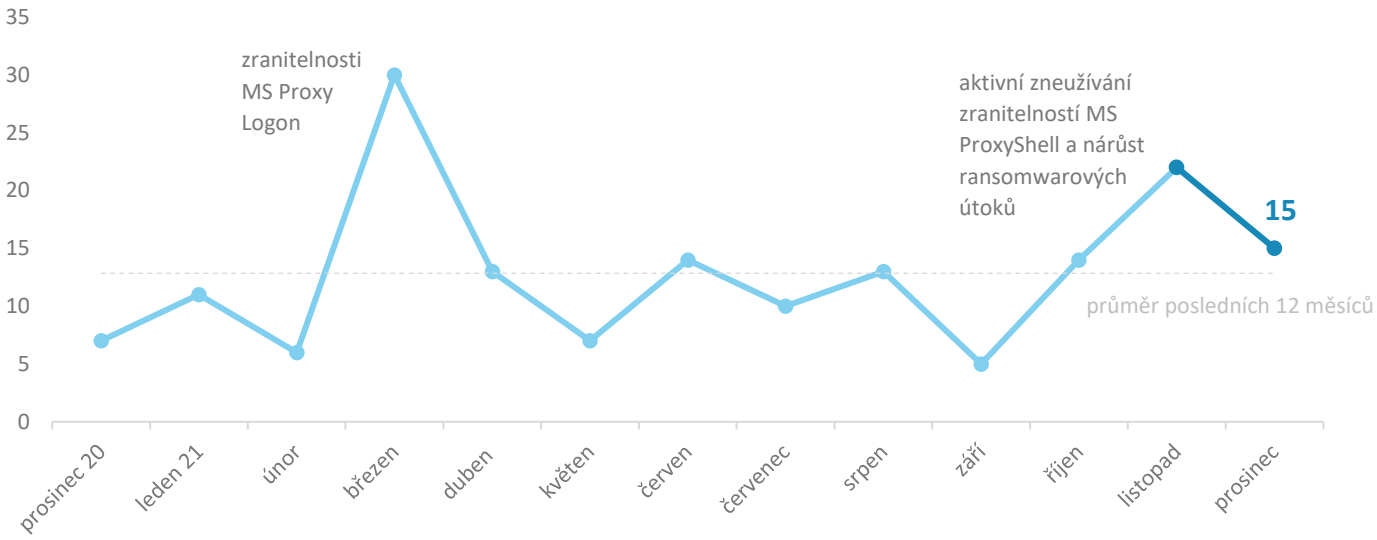
Obsah

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz.

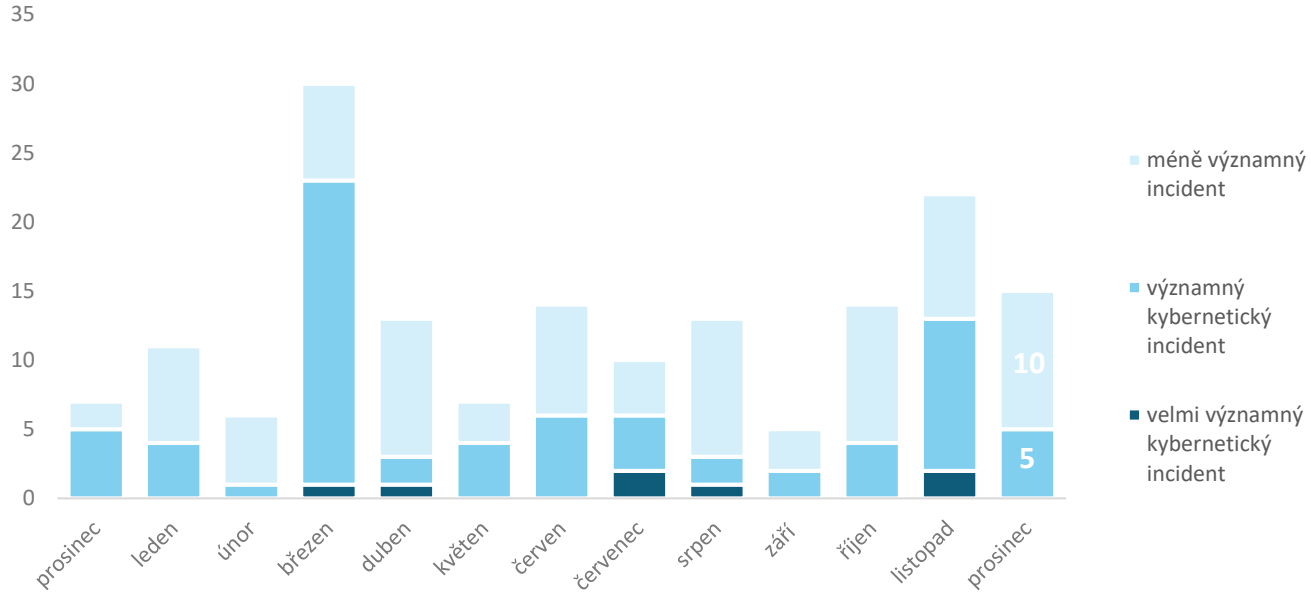
Počet kybernetických incidentů nahlášených NÚKIB

V porovnání s listopadem počet kybernetických incidentů v prosinci klesl o sedm. Vzhledem k nové zranitelnosti Log4Shell, která postihuje velké množství počítačových programů a aplikací, byl počet incidentů nižší, než jsme se po jejím zveřejnění obávali.[1]



Závažnost řešených kybernetických incidentů[2]

NÚKIB v prosinci neřešil žádný velmi významný incident, třetinu ze všech incidentů klasifikoval jako významné incidenty. Ty sice v některých případech omezily fungování napadených organizací, situaci se ale organizacím podařilo během krátké doby vyřešit a služby obnovit.



[1] Šest incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých devíti incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Obdobně jako v předchozích měsících stojí na prvních místech škodlivý kód a incidenty, které skončily nedostupností služeb. Mezi incidenty omezující dostupnost byl DDoS útok, technická chyba a ransomware, kdy dvě napadené organizace měly nedostatečně řešené zálohy a útok tak omezil jejich fungování. Ransomware se projevil i v kategorii škodlivý kód, jelikož ale oběť měla funkční zálohy, dostupnost jejích služeb neovlivnil. Dále se v této kategorii objevily nálezy řídících serverů malwarů a jeden incident spojený se zranitelností Log4Shell, kdy útočníci díky jejímu zneužití nainstalovali na webový server své oběti kryptominer (více ke zranitelnosti Log4Shell a s ní spojenými incidenty na str. 6).

[3] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu)

Trendy v kybernetické bezpečnosti za prosinec pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Po listopadu, kdy byly čtyři incidenty spojené se zranitelností ProxyShell úzce spjaty s phishigem, NÚKIB v prosinci řešil jediný, v rámci kterého neznámí útočníci kompromitovali e- mailový server jedné české státní organizace a dále z něj rozesílali podvodné zprávy v němčině.

Dvě české státní organizace pokusy o phishing zachytily, ale žádná kompromitace se u nich neprokázala.

Malware

Provozovatelé Emotetu, kteří se v listopadu vrátili na světovou i českou kybernetickou scénu, pokračovali ve své kampani. NÚKIB svou činností objevil dvě české organizace, jež Emotet kompromitoval a jejichž infrastruktury použil jako své kontrolní servery, ze kterých řídil další útoky.

NÚKIB v další české organizaci objevil také řídící server malwaru Dridex, který primárně cílí na bankovní údaje svých obětí.

Zranitelnosti

V prosinci rezonovala celým světem nově zveřejněná zranitelnost „Log4Shell“ s identifikátorem CVE-2021-44228, která potenciálně postihuje stovky miliónů zařízení a v jejímž důsledku mohou útočníci s minimem úsilí získat i plnou kontrolu nad systémy organizací. Vzhledem k závažnosti zranitelnosti NÚKIB vydal reaktivní opatření. Více informací naleznete na straně 6.

V prosinci se v ČR také stále ozývala kampaň MS ProxyShell. Jednalo se o stejný incident, který je popsaný výše ve phishingu.

Ransomware

Oproti předchozímu měsíci počet ransomwarových útoků klesl. Zatímco v listopadu NÚKIB řešil šest incidentů spojených s ransomwarem, v prosinci to byly tři. Jedna z napadených organizací měla funkční zálohy a obratem se jí podařilo znovu zprovoznit svou infrastrukturu. Zbylé dvě organizace zálohy plně funkční neměly a ransomware částečně omezil jejich fungování. Ransomwary, které v prosinci napadly české organizace, byly Phobos, BlackCat a Hive.

Útoky na dostupnost

Stejně jako v listopadu se v prosincových incidentech objevil pouze jeden DDoS útok. Ten se odehrál ve třech vlnách a v každé z nich způsobil napadené organizaci výpadek služeb na přibližně 15 minut.

[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

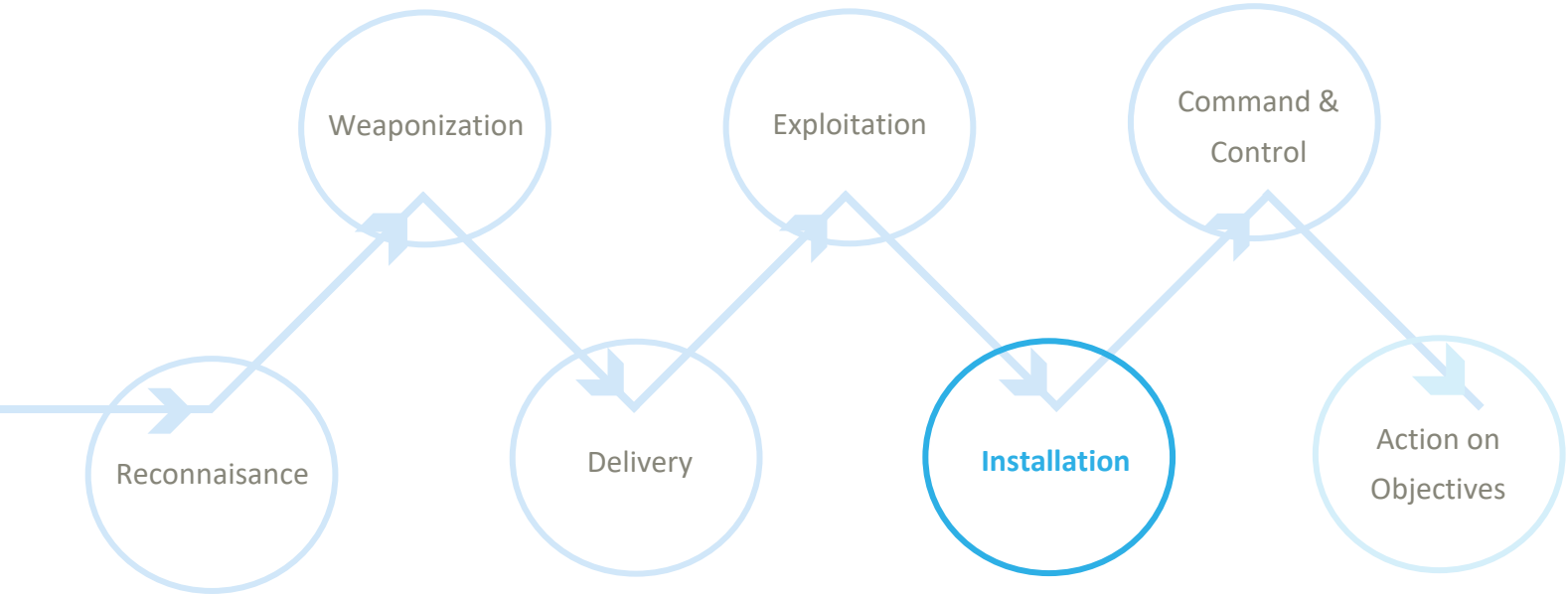
Nejpoužívanější technika měsíce: Process Injection

NÚKIB kybernetické incidenty vyhodnocuje také na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. NÚKIB na jeho základě mimo jiné určuje četnost využívání technik/taktik.

V prosincových incidentech se nejčastěji objevila technika, kterou MITRE nazývá „Data Encrypted for Impact“, kterou jsme popisovali v červencovém reportu. Aby se reporty neopakovaly, tato kapitola rozebere techniku „Process Injection“, která byla v prosinci druhou nejpoužívanější a která se objevila u incidentů spojených s Log4Shell, kdy útočníci nahrají kód do logovacího nástroje Log4j.

> **Process Injection** je technika, při níž útočníci přidají škodlivý kód do legitimních procesů v systému oběti. Pokud si uživatel spustí nástroj pro prohlížení spuštěných procesů, uvidí v něm pouze procesy, které jsou legitimní. Útočníci tím chtějí ztížit detekci jejich pohybu a zůstat tak v systému oběti nepozorováni. Příkladem Process Injection může být nahrání škodlivého kódu do procesu paměti prohlížeče, který oběť používá, do sdílených knihoven nebo jakéhokoliv jiného procesu, který běží v systému oběti.
>
> **MITRE ID: T1055**
>
> **Mitigace:** Některé nástroje pro detekci a reakce na útoky na koncová zařízení (např. EDR – Endpoint Detection & Response) lze nakonfigurovat tak, aby zachytily obecně známé kroky, které útočníci během Process Injection podnikají.

Znázornění „Process Injection“ v kill chainu, který ukazuje, ve které fázi útočníci techniku používají. V incidentech NÚKIB to odpovídalo Installation.



Zaměřeno na hrozbu: Log4Shell

Co je to Log4Shell?

Dne 9. prosince 2021 byla zveřejněna zranitelnost CVE-2021-44228, také známá jako Log4Shell. Tato zranitelnost se nachází v logovacím nástroji Log4j. Moderní softwary jsou složité programy, které tvoří velké týmy. Spíše, než aby je psaly řádek po řádku, dávají je dohromady z již existujících „stavebních bloků“. Log4j je jedním z nich. Autoři softwarů ho do svých produktů přidávají, aby mohli sledovat, co se v nich děje a řešit tak případné problémy. Většina dnešních softwarů má schopnost logovat a část z nich pro logování používá právě Log4j. Jedná se pravděpodobně o stovky miliónů systémů, aplikací a služeb, které Log4j používají, a jsou tím pádem potenciálně zranitelné.

Log4Shell je velmi závažná zranitelnost. Kód pro její zneužití je volně dostupný a je velmi jednoduchý. Útočník nemusí mít velké technické schopnosti, aby ho zvládl použít. Umožní mu ale téměř cokoliv. Útočníci díky němu mohou získat přístup do systémů svých oběti, mohou ukrást jejich přístupové údaje, data či instalovat další škodlivé kódy, včetně ransomwarů.

Jaká je situace ve světě?

Pár dní po zveřejnění zranitelnosti začalo ve světě její masivní zneužívání. Za většinou útoků, které pozoruje Microsoft Threat Intelligence Center (MSTIC), stojí skupiny provozující kryptominery nebo DDoS botnety. Nicméně MSTIC už potvrdil, že některé skupiny přístupy, které do sítí organizací díky Log4Shell získají, dále prodávají skupinám operujícím na bázi ransomware-as-a-service (RaaS). Podle MSTIC si kódy pro zneužití Log4Shell do svých toolboxů začali přidávat také aktéři zaštítění Čínou, Íránem, Tureckem nebo Severní Koreou. Je tak pravděpodobné (55–70 %), že větší útoky ze strany APT a ransomwarových skupin budou v následujících měsících na vzestupu.

Jaká je situace v ČR?

NÚKIB v prosinci řešil dva kybernetické incidenty spojené s Log4Shell. První organizace zachytila zneužívaní Log4Shell ve chvíli, kdy se útočník do jejich systémů snažil instalovat nástroj pro vzdálenou správu. V druhém případě nainstalovali útočníci skrze zranitelnost na webový server napadené organizace kryptominer. Vzhledem k rozšířenosti Log4Shell je ale téměř jisté (90-100 %), že napadených organizací je více než NÚKIB nyní eviduje.

2 kybernetické incidenty

5 % prokazatelně zranitelných organizací

NÚKIB nezná přesný počet zranitelných systémů, které se nachází v ČR. Jediné vodítko mu dávají skeny, které provedl na základě vydaného reaktivního opatření. Počet zranitelných strojů nelze zjistit pomocí nástroje Shodan, protože sken zranitelnosti Log4Shell je natolik intruzivní, že by se z něj stal de facto incident. Po vydání reaktivního opatření se NÚKIB přihlásily desítky organizací s žádostí o skenování jejich systémů. 5 % z nich bylo prokazatelně zranitelných vůči Log4Shell. Neznamená to ale, že by zbylých 95 % mělo své systémy zcela v pořádku. Většinu skenů NÚKIB zachytily technologie zabraňující skenování. Třetí strany tak nemohou jednoduše zjistit, jestli se v infrastruktuře těchto organizací zranitelné systémy nachází nebo ne. Sofistikovaný útočník by takové opatření dokázal obejít, ale proti plošným skenům, kdy se útočníci snaží objevit zranitelné systémy při co

nejmenším úsilí, jsou taková opatření účinná. NÚKIB navíc skenoval pouze perimetry organizací, uvnitř v infrastruktuře může být zranitelných strojů daleko více.

Doporučení

Jednotlivci

Log4j je součástí nástrojů a služeb, které každý z nás používá denně. Nejlepší, co mohou jednotlivci udělat, je neustále aktualizovat všechna svá zařízení a aplikace. Vývojáři je od zveřejnění zranitelnosti postupně opravují.

Organizace

Organizacím NÚKIB doporučuje, aby se řídily kroky k zabezpečení systémů, které jsou uvedeny v reaktivním opatření ze dne 15. prosince 2021.

Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit/Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to--know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:WHITE	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.