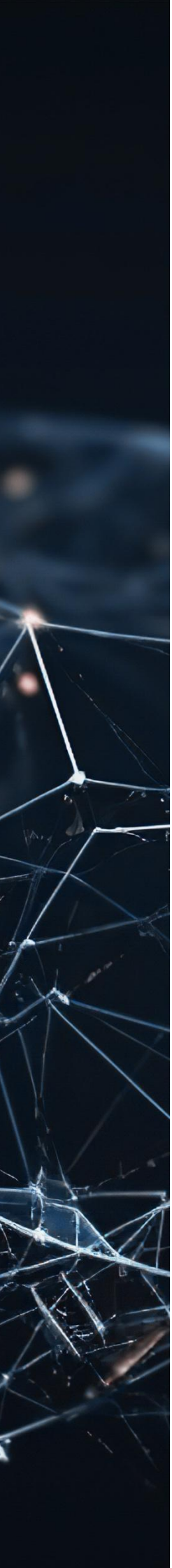


Spolufinancovaný Európskou úniou

PROGRAM SLOVENSKO

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Všeobecné informácie o systéme ACHILLES od VJ CSIRT

ACHILLES

Verzia: 1.5

TLP:CLEAR

O službe Achilles

Vládna jednotka CSIRT („VJ CSIRT“) ako súčasť Ministerstva investícií regionálneho rozvoja a informatizácie SR („MIRRI“) je v súlade so zákonom č. 95/2019 Z.z. o informačných technológiách verejnej správy v platnom znení, oprávnená vykonávať pravidelné neinvazívne hodnotenie zraniteľností služieb verejnej správy poskytovaných cez internet alebo prostredníctvom vládnej siete, Govnet. Výsledky sú následne vyhodnocované a oznamované správcovi. VJ CSIRT môže vykonať detailné hodnotenie zistených zraniteľností so súhlasom správcu.

Registráciou do systému Achilles získate:

1. Každý mesiac Vám odošleme **report zraniteľností**, ktoré sa nachádzajú na Vašich verejných IP adresách. Na **odšifrovanie** prijatej správy odporúčame využiť **externú aplikáciu**, napr. 7-Zip alebo WinRAR, keďže natívny Windows má problémy s rozbaľovaním archívov podporujúcich moderné štandardy pre šifrovanie. Skenovanie zraniteľností z kapacitných dôvodov vykonávame automatizovaným skenerom (vykonáva sa plošne) a jeho cieľom je odhaliť najznámejšie druhy zraniteľností. V prípade záujmu o **kompletné penetračné testovanie aplikácií** je možné požiadať o službu Ares, podľa pokynov v informačnom liste. Manuálne overovanie (validácia) kritických zraniteľností sa v súčasnosti vykonáva len na základe konkrétnej žiadosti organizácie a to v prípade dostatočných kapacít VJ CSIRT, keďže skenovaných systémov sú tisíce. VJ CSIRT má právo rozhodnúť, akým spôsobom, v akom rozsahu a v akom poradí bude poskytovať svoje služby.
2. Získate informácie o **aktívne zneužívaných zraniteľnostiach**; pokiaľ VJ CSIRT deteguje potenciálne zraniteľné služby na Vašich verejných IP adresách, pošleme Vám varovanie alebo odporúčanie.
3. **Odporúčania** pre zabezpečenie Vašej siete vyplývajúce z identifikovaných nálezov, ak sa na Vašich verejných IP adresách nachádzajú potenciálne zneužiteľné služby.

TLP:CLEAR

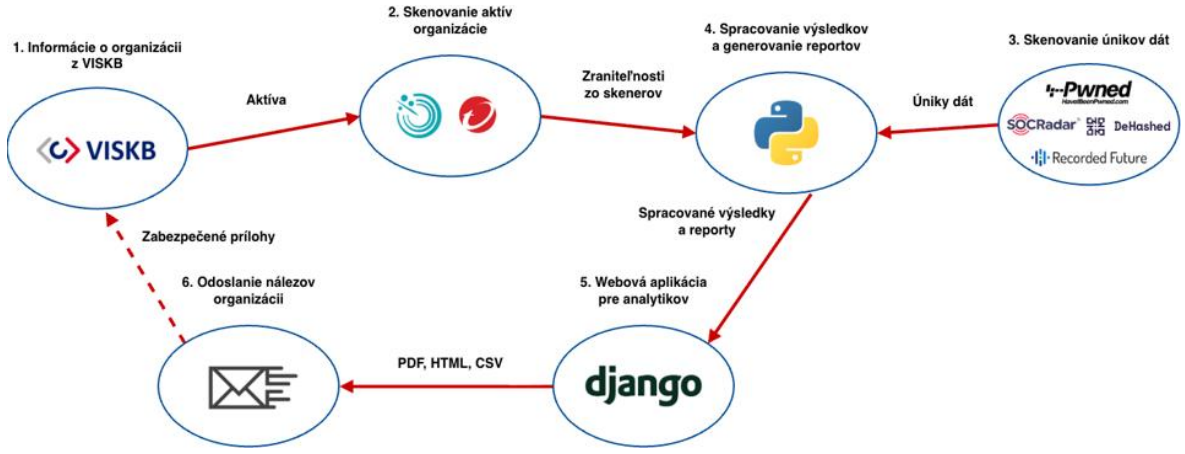
4. **Detekciu technológií** webových služieb prostredníctvom modulu **Domino**. Táto informácia je východisková **pre Hermes (Systém včasného varovania)**.

Systém Achilles ako služba vyhľadávania zraniteľností

VJ CSIRT prevádzkuje systém **Achilles**, ktorý bol vybudovaný na **centralizované riadenie zraniteľností** z pohľadu aktéra hrozieb útočiaceho z prostredia verejného internetu. V systéme Achilles VJ CSIRT získava a spracováva informácie o zraniteľnostiach, informuje inštitúcie o zraniteľnostiach, ktoré sú **je možné detegovať** z prostredia verejného internetu. Bližšie informácie nájdete v príslušnej sekcii na oficiálnom **webovom sídle VJ CSIRT.** Súčasťou systému Achilles je aj modul **Domino,** ktorý slúži pre monitoring dostupnosti verejne dostupných webových služieb, teda ako systém včasného odhaľovania útokov typu DoS/DDoS alebo technických výpadkov.

Systém Achilles má za úlohu **znížiť riziko zneužitia potenciálnych vektorov útokov** na infraštruktúry organizácií/subjektov verejnej správy a tým cielene **znižovať pravdepodobnosť vzniku závažných kybernetických bezpečnostných incidentov**. Ďalšou úlohou systému je poskytovať včasné varovania na známe hrozby**.**

Systém Achilles sa skladá z proprietárneho programového vybavenia aj vlastného programového vybavenia, v podobe analytickej platformy, nad ktorou pracuje aplikácia (tzv. Cyber Operations Center, COC) VJ CSIRT pre ukladanie, filtrovanie a spracovávanie dát subjektov štátnej a verejnej správy. Zjednodušenú architektúru systému Achilles znázorňuje Obrázok *1*.



Obrázok 1: Architektúra služby Achilles

Schopnosti systému Achilles

Pre lepšie pochopenie prínosov systému Achilles je potrebné definovať, čo **systém** Achilles **dokáže:**

1. **Automatizovaná detekcia známych zraniteľností v rámci externej infraštruktúry aj na webovom serveri.** Proaktívne automatizované skenovanie zraniteľností na webových serverov pre organizácie, ktoré udržiavajú aktuálny zoznam kontaktov a aktív **vo Vládnom informačnom systéme kybernetickej bezpečnosti (VISKB).**
2. **Kontrola verejne dostupných portov a služieb.** Odhaľovanie verejne dostupných portov a služieb, ktorých dostupnosť by mohla predstavovať bezpečnostnú hrozbu pre danú organizáciu.
3. **Mesačné skenovanie a odosielanie reportov.** Spúšťanie mesačných automatizovaných bezpečnostných skenov na overenie zabezpečenia serverov a webových služieb pre jednotlivé organizácie, ktoré udržiavajú aktuálny zoznam kontaktov a aktív **vo Vládnom informačnom systéme kybernetickej bezpečnosti (VISKB).**
4. **Upozornenie na potenciálne zraniteľné prvky v infraštruktúre.** Overovanie prítomnosti novej zraniteľnosti, ktorá by mohla predstavovať hrozbu pre organizáciu v našej konštituencii, automatom.
5. **Detekcia jednotlivých technológií webových aplikácií (modul Domino).** Táto informácia je východiskové pre Systém včasného varovania.

Pre lepšie pochopenie prínosov systému **Achilles** je potrebné definovať aj čo systém Achilles (resp. podobné riešenia s cieľom centralizovaného riadenia zraniteľností) **nedokáže**[1]**:**

1. **Odhaliť všetky zraniteľnosti.** Aj keď systém Achilles Vás dokáže upozorniť na mnohé známe zraniteľnosti (z pohľadu útočníka, ktorý cieli na perimeter organizácie), keďže nie je invazívny, existujú zraniteľnosti (na ich odhalenie je potrebné byť prihlásený

[1] O niektoré z týchto služieb je možné požiadať v rámci aktuálneho Katalógu služieb VJ CSIRT

do daného systému) a bezpečnostné nastavenia (napríklad slabá politika hesiel alebo rovnaké jednoduché heslo do služieb nezmenené už niekoľko rokov), ktoré nedokáže plošné neinvazívne skenovanie zraniteľností odhaliť. Na odhalenie čo najväčšieho počtu zraniteľností a nedostatkov v rámci kybernetickej bezpečnosti zariadení slúži práve **penetračné testovanie** poskytované prostredníctvom služby **Ares.**

2. **Vykonať penetračné testovanie.** V prípade záujmu o objavenie čo najväčšieho počtu zraniteľností, a teda invazívne testovanie vybraných informačných systémov, je možné požiadať aj o vykonanie penetračného testovania podľa pokynov informačných listov služby **Ares.** Penetračné testovanie je v závislosti od rozsahu testovania zdĺhavý proces, ktorý je potrebné vykonať manuálne doménovým expertom.

3. **Vykonať riadenie záplat.** Systém Achilles bol vybudovaný na **centralizované riadenie zraniteľností**, avšak neposkytuje (a ani nemôže) funkcionalitu riadenia záplat (angl. Patch Management). Inštaláciu záplat a opravu zraniteľností alebo zníženie rizika je na zodpovednosti organizácie odberajúcej službu hodnotenia zraniteľností, buď vlastnými silami alebo požiadavkou u svojho dodávateľa, s ktorým má podpísanú platnú dohodu. V rámci systému Achilles však môže organizácia požiadať o opätovné skenovanie, či bola zraniteľnosť opravená alebo je možné poskytnúť odbornú pomoc pri odstraňovaní zraniteľnosti, podľa kapacitných možností Vládnej jednotky CSIRT. **Odstraňovanie identifikovaných zraniteľností je vždy zodpovednosťou organizácie**.

4. **Skenovať bez súčinnosti organizácie.** Systém Achilles (ani podobné systémy hodnotenia zraniteľností) nemôže skenovať perimeter organizácií verejnej správy bez dostatočnej súčinnosti. Podmienkou poskytovania služby Achilles je **pravidelná aktualizácia kontaktov a najmä aktív dostupných z internetu alebo siete Govnet** v rámci **Vládneho informačného systému kybernetickej bezpečnosti (VISKB).**

Modul Domino

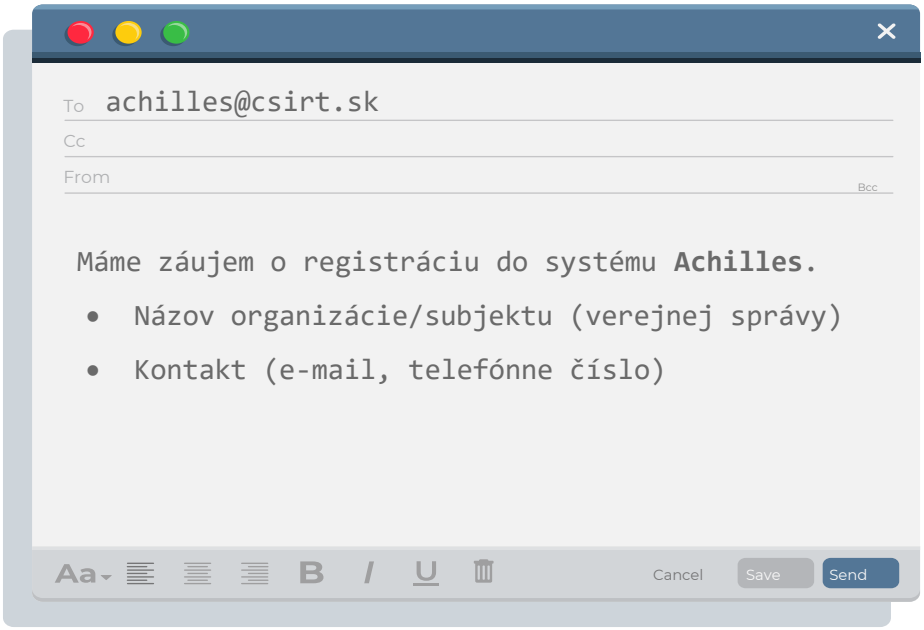
Modul **Domino** má v systéme Achilles na starosti skenovanie webových služieb, ktoré si organizácia definuje s cieľom získať prehľad o dostupnosti a využitých webových technológiách (kľúčový prvok pre Hermes). Dostupnosť sledovanej webovej lokality je overovaná cez odosielanie **GET požiadaviek** na porty 80 (HTTP) a 443 (HTTPS). Frekvencia týchto požiadaviek je min. každých 30 minút (ak je aktívum dostupné) a max. každých 15 minút (ak je aktívum nedostupné). Zaručuje sa tak kontinuálne overovanie dostupnosti určených aktív bez ohľadu na ich aktuálny stav.

Pripomíname, že na poskytovanie služieb modulu Domino je nutné, aby si správca nastavil svoju infraštruktúru tak, aby nedošlo k automatickému blokovaniu požiadaviek z modulu Domino, resp. z verejnej IP adresy, odkiaľ Domino posiela požiadavky. Bližšie informácie k tejto požiadavke vieme poskytnúť v procese registrácie do systému Achilles.

Požiadavky na registráciu do systému Achilles

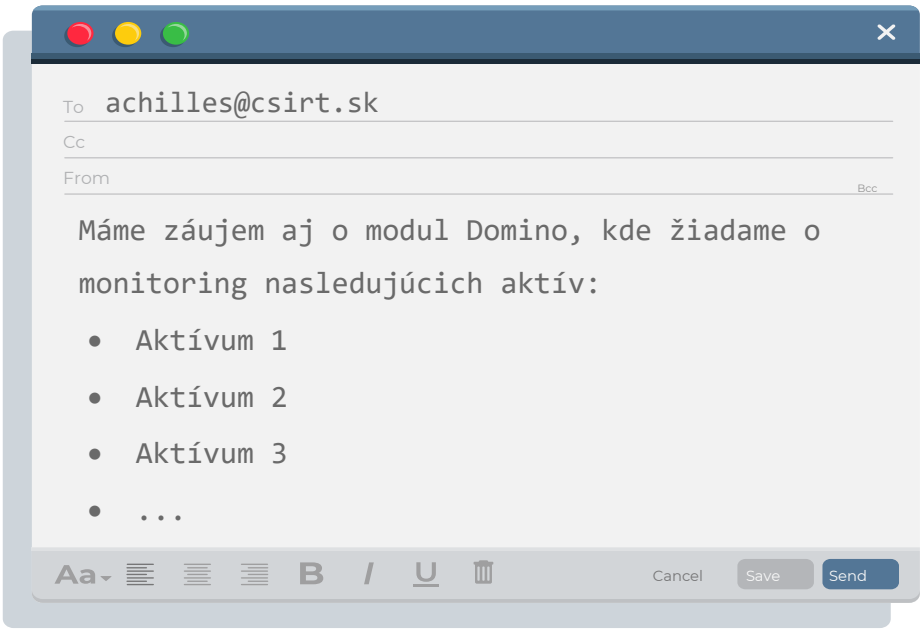
Systém Achilles je poskytovaný konštituencii VJ CSIRT, resp. organizáciám, ktoré spadajú do verejnej správy, čo je aktuálne jedinou podmienkou na prijatie požiadavky o registráciu do systému Achilles.

V rámci registrácie nás treba kontaktovať na e-mailovej adrese **achilles@csirt.sk** s nasledujúcim textom:



TLP:CLEAR

Ak máte záujem aj o služby modulu Domino, do e-mailu pridajte aj nasledujúci text s uvedenými aktívami[2]:



Po úspešnom prijatí e-mailovej žiadosti Vám vytvoríme prístup k systému VISKB pre registráciu informácií o Vašej organizácii. V systéme Vás požiadame o zaznamenanie informácií o Vašej infraštruktúre, ktorá bude predmetom pravidelného monitoringu zraniteľností a dostupnosti z verejného internetu.

[2] *Aktíva nemusia byť určené samostatne, môže ísť aj o skupinu aktív, ako napr. celý subnet.*

Často kladené otázky

Podobnosť s reálnymi otázkami odberateľov služby je čisto náhodná. Ak by ste našli niektoré z vlastných výrokov, ide o len o zhodu náhod a nie o doslovný prepis.

1. **Bojíme sa, že keď sa zapojíme do služby Achilles, tak budete vedieť o našich zraniteľnostiach a pošlete na nás kontrolu.**

   Cieľom systému Achilles nie je posielať kontroly, ale podporiť odolnosť Vašej organizácie voči stále sa vyvíjajúcim kybernetickým hrozbám. V prípade existencie kritickej alebo vysokej zraniteľnosti je potrebné ju odstrániť bezodkladne (aj zo systémov, ktoré spracuje Váš dodávateľ, nie interný tím, dokonca aj z nepoužívaných systémov). V prípade, ak na toto Váš tím nestačí, môžete túto skutočnosť komunikovať ako odpoveď na konkrétne nálezy so žiadosťou o usmernenie alebo súčinnosť. Radi Vám ju v rámci našich kapacitných možností poskytneme. Máme na starosti ale viac ako 8000 organizácií, preto môže pár dní, kým sa k žiadosti dostaneme.

2. **Bojím sa, že budem mať problémy, ak bude Vládna jednotka vedieť o zraniteľnostiach na mojom perimetri.**

   Aj najlepší softvér na svete a aj ten najlepší tím na svete sa stretne s výskytom zraniteľností. Systém Achilles pomôže organizácii odhaliť zraniteľnosti z pohľadu útočníka z verejného internetu a teda je pre organizáciu odberajúcu službu Achilles cenným zdrojom informácií. Čo je ale úplne v rukách organizácie, je spôsob, akým sa postaví k zníženiu rizika zneužitia zraniteľnosti. Vládnej jednotke pomôžu informácie na včasné varovania organizácie (podľa princípu „poznaj svojho zákazníka“) a zároveň na ďalšie smerovanie svojich služieb voči organizácii a vnímanie kontextu, v prípade pomoci pri riešení incidentov alebo zraniteľností.

3. **Chýbajú nám finančné možnosti na zakúpenie tejto služby** 😟

   To nevadí, mysleli sme aj na Vás. Služby VJ CSIRT sú poskytované organizáciám verejnej správy bezodplatne. Aktuálny prehľad služieb poskytovaných jednotkou nájdete v **Katalógu služieb Vládnej jednotky CSIRT**.

4. My síce máme kritické a vysoké zraniteľnosti, ale systém už nepoužívame, žiadne riziko nehrozí, ďakujeme za informáciu jednotke CSIRT.

   Práve nepoužívane a neudržiavané systémy sú často pre útočníkov vstupnou bránou do Vašej internej infraštruktúry. Väčšina incidentov, ktoré sme v rámci VJ CSIRT riešili mala práve jeden zo vstupných vektorov neudržiavaný systém. Achilles nie je ale jediným zdrojom informácii o zraniteľnostiach pre Vašu organizáciu, viac sa dočítate v rámci **Systému včasného varovania**.

5. Už sme v službe Achilles a ideme opraviť všetkých 120 zraniteľností !

   Cieľom riadenia zraniteľností nie je opraviť všetky zraniteľnosti (veď každý mesiac Vám môžu pribudnúť nové), ale doručiť k Vám informáciu o prehľade zraniteľností detegovaných z internetu podľa závažnosti. Je na organizácii, aby identifikovala kritické systémy a priorizovala zraniteľnosti.

6. Formát správ o zraniteľnostiach sa každý mesiac mení, takto sa nedá pracovať !!!

   V súčasnosti náš tím usilovne pracuje na vývoji systémov Achilles 2.0 a Vládny informačný systém 2.0, pretože vnímame spätnú väzbu od organizácií a chceme pripomienky zapracovať a službu zlepšovať a rozširovať. Preto sa mohlo stať, že boli odosielané rôzne formy reportov, vzhľadom na veľkosť a kapacity tímu.

7. Bojím sa, že Vaše skenovanie mi spomalí systém a naše služby budú nedostupné a to nechceme, budeme mať problémy.

   Frekvencia dopytov a rýchlosť skenovania sa prispôsobuje systémom, aby nebolo možné ich zahltiť, preto nie je potrebné systémy dať do režimu údržby (angl. maintenance mode). V prípade, ak by ste identifikovalo, že zdrojové IP adresy systému Achilles posielajú počas skenovanie príliš veľké množstvo požiadaviek, je potrebné to komunikovať aj s príslušnými dôkazmi svojich tvrdení s časovou pečiatkou.

8. Ako prebieha overenie úniku prihlasovacích údajov?

   Na základe zoznamu domén, ktoré poskytne organizácia, je možné detegovať úniky prihlasovacích údajov zaznamenané v nasledujúcich zdrojoch: Have I Been Pwned, Recorded Future, SOCRadar a DeHashed. Zdetegované úniky sú organizácii

odosielané na dennej báze. V súčasnosti môžete dostať aj staré úniky alebo duplicity, snažíme sa však tieto prípady minimalizovať.

9. Zhodili ste nám infraštruktúru a zahltili databázu, takéto podmienky neboli dohodnuté.

   V prípade, ak máte podozrenie, že došlo k porušeniu podmienok služby Achilles, je potrebné to bezodkladne nahlásiť aj s príslušnými dôkazmi na **achilles@csirt.sk** s predmetom ACHILLOVA PATA: [Téma]. A to detailným opisom situácie a priložením logov na analýzu vzniknutého problému.

10. Chceme workshopy, chýbajú nám informácie, ako máme pracovať s reportom a čo očakávať od služby Achilles a takisto nikde nevidím nové VISKB.

    Všetky vyššie spomenuté nedostatky dlhodobo vnímame aj na strane VJ CSIRT. Robíme všetko, čo je v našich silách, aby sme tieto nedostatky odstránili. Tu môžeme len odporučiť, aby ste sledovali **webové sídlo VJ CSIRT**, boli registrovaní **v systéme VISKB**, prípadne sledovali naše sociálne siete (**LinkedIn**, **Facebook**, **X** alebo v budúcnosti **GitHub**). Čakanie si môžete skrátiť zábavnou formou v rámci **Kyberbezpečnostnej hry: Fakt alebo mýtus**. Na dokončení **nového VISKB** a migrácii údajov v súčasnosti intenzívne pracujeme.

11. Máme veľmi veľa zraniteľností na serveroch, nie sú až také závažné, ale je potom strašne dlhý ten report, ty kokos.

    Množstvo zraniteľností je možné opraviť jednoduchou inštaláciou záplat alebo počiatočnou konfiguráciou, ktorú môžete vyžadovať od dodávateľa. Napríklad, v našej knižnici nájdete návody na hardening: **Wordpress**, **Nginx, Apache**, **Unattended Upgrades**.

12. Chcel by som prispieť k rozvoju systému Achilles, je to podľa mňa najlepšia vec na svete. 😊

    Ďakujeme, počúvame to veľmi často 😉. Stačí svojou troškou prispieť detailným návrhom na **achilles@csirt.sk**, s predmetom CHCEM POMOCT: [Téma]

Kontaktné údaje

V prípade otázok na systém Achilles a poskytovanie tejto môžete kontaktovať VJ CSIRT na e-mailovej adrese **achilles@csirt.sk.** Denne dostávame množstvo správ, pričom sektor VJ CSIRT zahŕňa viac ako 8000 subjektov verejnej správy, odpoveď na Vaše otázky môže chvíľu trvať. Stále však môžete využiť aj telefonický kontakt na preverenie stavu Vašej požiadavky.

Ďalšie zdroje informácií o službe Achilles

1. Slovakian Lessons On Proactive Cybersecurity & Vulnerability Disclosure
2. Prezentácia systému Achilles na konferencii OSCP 2024