SŽ PRAVIDLA PRO HLAŠENÍ ZRANITELNOSTÍ

ZÁSADY PRO ZVEŘEJŇOVÁNÍ INFORMACÍ O ZRANITELNOSTECH SPRÁVY ŽELEZNIC, S.O.

SŽ PRAVIDLA PRO HLÁŠENÍ ZRANITELNOSTÍ
ZÁSADY PRO ZVEŘEJŇOVÁNÍ INFORMACÍ O ZRANITELNOSTECH SPRÁVY ŽELEZNIC, S.O.

Gestorský útvar: Správa železnic, státní organizace
Správa železniční telematiky
Úsek kybernetické bezpečnosti
Praha
spravazeleznic.cz
Rok vydání: 2023
Náklad: Vydáno pouze v elektronické podobě, formát A4

ZÁZNAMY O OPRAVÁCH A ZMĚNÁCH

Držitel listinné podoby tohoto dokumentu je odpovědný za včasné a správné zapracování účinných oprav a změn a za provedení příslušného záznamu.

Oprava/změna a její pořadové číslo	Číslo jednací	Účinnost od	Opravu/změnu zapracoval

OBSAH

ZKRATKY A ZNAČKY

Níže uvedený seznam obsahuje zkratky a značky použité v tomto dokumentu. V seznamu se neuvádějí legislativní zkratky, zkratky a značky obecně známé, zavedené právními předpisy, uvedené v obrázcích, příkladech nebo tabulkách.

CSIRT .....Computer Security Incident Response Team

DDoS .....Distributed Denial of Service

DIČ.....Dnové identifikační číslo

DoS .....Denial of Service

FIRST.....Fórum CISRT týmů pro reakci na incidenty a bezpečnost

IČO.....Identifikační číslo

ID.....Identification

NÚKIB.....Národní úřad pro kybernetickou a informační bezpečnost

PDF.....Portable Document Format

Phishing .....Útok pomocí sociálního inženýrství, kdy se útočník snaží získat důvěrná data oběti nebo spustit na zařízení oběti škodlivý kód.

s.o.....Státní organizace

SELČ.....Středoevropský letní čas

SOC.....Security Operations Center

SZ .....Správa železnic

SZT .....Správa železniční telematiky

Tailgating .....typ narušení fyzické bezpečnosti, při kterém neoprávněná osoba sleduje oprávněnou osobu, aby vstoupila do zabezpečených prostor

TI .....Trusted Introducer

UTC .....Coordinated Universal Time

Vishing.....Útok pomocí sociálního inženýrství je typ phishingového útoku, který používá hlasový hovor a techniky sociálního inženýrství.

1 ÚVODNÍ USTANOVENÍ

1.1 **Pravidla pro hlášení zranitelností**

Pravidla pro hlášení zranitelností (dále jen „**Pravidla**") Správy železnic, státní organizace se sídlem Dlážděná 1003/7, 110 00 Praha 1 – Nové Město, IČO 70 99 42 34, DIČ CZ70994234 zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A, vložka 48384 představují soubor zásad pro zveřejňování informací o zranitelnostech Správy železnic, s.o.

2 ZÁSADY PRO ZVEŘEJŇOVÁNÍ INFORMACÍ O ZRANITELNOSTECH

2.1 Pro Správu železnic, s.o. (dále jen „SŽ") je důležitá bezpečnost cestujících, zákazníků a dalších, a to v oblasti ochrany dat, informací a osobních údajů. V rámci zajištění vysoké úrovně informační a kybernetické bezpečnosti informačních systémů SŽ je zaveden proces pro zveřejňování zranitelností. Účelem těchto zásad je podpořit odpovědné a bezpečné hlášení zranitelností, které jsou zjištěny v informačních systémech SŽ.

2.2 **Datum poslední aktualizace**
Tento dokument je první verzí ze dne 27.07.2023

2.3 **Distribuční seznam pro oznámení**

Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu CSIRT SZ, **soc@spravazeleznic.cz**.

2.4 **Dostupnost dokumentu**
Aktuální verze tohoto dokumentu je dostupná na webových stránkách:

https://www.spravazeleznic.cz/o-nas/kyberneticka-bezpecnost/csirt

3 KONTAKTNÍ INFORMACE

3.1 **Název týmu**
CSIRT SZ, tedy Computer Security Incident Response Team Správy železnic, s.o.

3.2 **Adresa**
CSIRT SZ
V Celnici 1028/10
110 00 Praha 1
Česká republika

3.3 **Časové pásmo**
Středoevropský čas (UTC +1, od poslední neděle v říjnu do poslední neděle v březnu) SELČ, Středoevropský letní čas (UTC +2, od poslední neděle v březnu do poslední neděle v říjnu).

3.4 **Telefonní číslo**
+420 **972 235 333** (linka je dostupná 24/7/365).

3.5 **Ostatní telekomunikace**
Žádné.

3.6 **Elektronická adresa**
Oznámení (hlášení) incidentu zasílejte na e-mailovou adresu **soc@spravazeleznic.cz**. Na obdržený e-mail je odpovězeno ve většině případů do 12 hodin.

3.7 **Veřejné klíče a informace o šifrování**
CSIRT SZ podepisuje odchozí elektronické zprávy. Kromě toho provádí CSIRT SZ dešifrování obdržených e-mailových zpráv a ověřuje, zda je digitální podpis zprávy validní.

Pro oznámení (hlášení) incidentu a související komunikaci prosím využijte níže uvedený klíč. Komunikační klíč (použijte pro ověření a šifrování):

- **User ID:** SŽ SOC <**soc@spravazeleznic.cz**>
- **Key ID:** D7DD CFAA 3C5D 46E1
- **Fingerprint:** E1A5 18B9 95FB 2E00 2727 9566 D7DD CFAA 3C5D 46E1

3.8 **Další informace**

Obecné informace o CSIRT SZ lze nalézt na webových stránkách sdružení Trusted Introducer (dále jen „**TI**").[1]

3.9 **Kontakt s veřejností**

Preferovaný způsob kontaktování CSIRT SZ je prostřednictvím e-mailu. Oznámení (hlášení) incidentů a související otázky by měly být zaslány na e-mailovou adresu **soc@spravazeleznic.cz**. Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, obracejte se na CSIRT SZ telefonicky.

4 ROZSAH PŮSOBNOSTI

Tyto zásady se vztahují na veškeré systémy a aplikace vlastněné nebo provozované SŽ, včetně webových stránek, webových aplikací a aplikačního programového rozhraní.

4.1 **Povolený rozsah testování**

Všechny možnosti testování jsou povoleny s výjimkou těch, které omezují nebo brání funkčnosti systému.

Následující zkušební metody nejsou povoleny:

- Testy (DoS nebo DDoS) nebo jiné testy, které zhoršují přístup k systémům, datům nebo je jiným způsobem poškozují.
- Fyzické testování (např. přístup do kanceláře, otevřené dveře, tailgating), sociální inženýrství (např. phishing, vishing) nebo jiné netechnické testování zranitelnosti.
- Úplné penetrační testování, které zahrnuje neoprávněný přístup k serverům.

4.2 **Hlášení zranitelnosti**

Informace poskytnuté podle těchto zásad budou použity pouze pro obranné účely a zejména pro zmírnění nebo nápravě zjištěné zranitelnosti.

Pokud vaše zjištění obsahují nově objevené zranitelnosti, které se týkají např. uživatelů SŽ či produktu nebo služby SŽ, bude hlášení poskytnuto Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB").

Bez výslovného souhlasu nebudeme sdílet vaše jméno ani kontaktní údaje. Správa železnic, s.o. přijímá pouze výstupní zprávy z testování zranitelností, a to ve formě Portable Document Format (PDF). Žádný jiný formát nebude společností akceptován a považován za platný.

Samotná zpráva musí obsahovat následující:

- Popis místa, kde byla zranitelnost objevena s popisem potenciálního dopadu zneužití.
- Podrobný popis jednotlivých kroků, jenž umožní reprodukci útoku.
- Preferované znění zprávy jsou v českém či anglickém jazyce.

Odpovědi na Vámi zaslané výstupní zprávy či jiné dotazy nejsou automatické. Bezpečnostní tým CSIRT SZ přezkoumává všechny obdržené zprávy a v co nejkratším čase na ně reaguje, nejpozději však do jednoho pracovního dne po obdržení. CSIRT SZ neodpovídá na stížnosti nebo dotazy, jelikož to není předmětem tohoto dokumentu.

[1] Dostupné z https://www.trusted-introducer.org/

4.3 **Finanční ohodnocení**

Správa železnic, s.o. neposkytuje oznamovatelům za zaslání zjištěné zranitelnosti žádné finanční odměny. Oznamovatelé, kteří zranitelnost předkládají pomocí zprávy, se tímto automaticky vzdávají jakýchkoli nároků na odměnu.