

SALUS Controls PLC - Formulář pro hlášení podezření na zranitelnost

Tento formulář použijte k nahlášení podezření na bezpečnostní zranitelnost, která se týká produktu, aplikace, cloudové služby nebo webových stránek SALUS.

Vyplňte prosím co nejvíce informací. Abychom vaše hlášení přijali, nemusíte vyplnit všechna pole. Hlášení můžete podat anonymně. Pokud však neuvedete kontaktní údaje, nemusíme být schopni vyžádat si doplňující informace ani vás informovat o průběhu řešení vašeho hlášení.

Po vyplnění zašlete tento formulář na adresu security@saluscontrols.com.

Neuvádějte prosím hesla, autentizační tokeny, soukromé klíče ani zbytečné osobní údaje či údaje zákazníků.

Pole označená jako „Povinné“ jsou povinná pouze tehdy, pokud jsou dané informace přiměřeně dostupné. Hlášení můžete odeslat i v případě, že nemáte všechny informace.

Hlášení podezření na zranitelnost

1. Údaje o oznamovateli

Pole	Odpověď
Jméno nebo alias (volitelné)	
Organizace (volitelné)	
E-mail / způsob kontaktu (povinné, pokud nehlásíte anonymně)	
Preferovaný jazyk (volitelné)	
Hlásíte anonymně?	☐ Ano ☐ Ne

2. Dotčený produkt nebo komponenta

Pole	Odpověď
Název produktu nebo služby (povinné)	
Model (je-li relevantní)	
Verze hardwaru (je-li známa)	
Verze firmwaru / softwaru / aplikace (je-li známa)	
Země / region	
Další relevantní informace o konfiguraci	

3. Popis podezření na zranitelnost

Pole	Odpověď
Krátký název (povinné)	
Popište prosím zjištěný bezpečnostní problém (povinné)	
Kdy jste problém poprvé zaznamenali?	
Co jste očekávali, že se stane?	
Co se skutečně stalo?	
Dokážete problém reprodukovat?	☐ Ano ☐ Ne ☐ Někdy ☐ Neznámé
Pokud je to možné, popište kroky potřebné k reprodukci:	
Jaký bezpečnostní dopad by podle vás mohl problém mít?	
Jsou přiloženy přílohy? Můžete přiložit relevantní snímky obrazovky, protokoly, videa nebo informace proof of concept.	☐ Ano ☐ Ne

Doplňující technické informace (volitelné – pro bezpečnostní výzkumníky)

Pole	Odpověď
Typ zranitelnosti (obejití autentizace, injection, poškození paměti apod.), je-li znám	
CWE / CVE, je-li známo	
Technická příčina / podrobnosti	
Testovací prostředí / konfigurace	
Ověření konceptu	

4. Scénář útoku

Scénář útoku se liší od postupu pro reprodukci problému. Popište, jak by mohl reálný útočník tuto zranitelnost zneužít.

Pole	Odpověď
Je-li známo, popište prosím, jak by někdo mohl tuto zranitelnost zneužít	
Přístup útočníka	☐ Vzdálená síť ☐ Sousední síť ☐ Místní síť ☐ Místní zařízení ☐ Fyzický přístup ☐ Neznámé
Vyžadována interakce uživatele	☐ Ano ☐ Ne ☐ Neznámé
Vyžadována zvláštní oprávnění / účet	☐ Ano ☐ Ne ☐ Neznámé Pokud ano, popište požadovaná oprávnění / účet:

5. Posouzení dopadu (volitelné)

Tuto část vyplňte, pokud dokážete posoudit možný dopad.

Oblast dopadu	Posouzení oznamovatele
Důvěrnost	☐ Nene ☐ Nízký ☐ Střední ☐ Vysoký ☐ Neznámé
Integrita	☐ Nene ☐ Nízký ☐ Střední ☐ Vysoký ☐ Neznámé
Dostupnost	☐ Nene ☐ Nízký ☒ Střední ☐ Vysoký ☐ Neznámé
Bezpečnost	☐ Nene ☐ Nízký ☐ Střední ☐ Vysoký ☐ Neznámé
Soukromí	☐ Nene ☐ Nízký ☐ Střední ☐ Vysoký ☐ Neznámé
Dopad na dodavatelský řetězec nebo širší ekosystém	☐ Žádný ☐ Nízký ☐ Střední ☐ Vysoký ☐ Neznámé
Navrhovaná závažnost, je-li k dispozici (volitelné)	☐ Nízký ☐ Střední ☐ Vysoký ☐ Kritická ☐ Neznámé
Vektor CVSS, je-li k dispozici (volitelné)	

6. Stav zneužití a zveřejnění

Pole	Odpověď
Je zranitelnost již veřejně známá?	☐ Ne ☐ Ano ☐ Neznámé Pokud ano, uveďte URL a datum:
Je proof of concept veřejně dostupný?	☐ Ne ☐ Ano ☐ Neznámé Pokud ano, uveďte URL a datum:
Je známo nebo existuje podezření na aktivní zneužívání?	☐ Ne ☐ Ano ☐ Neznámé Pokud ano, uveďte podrobnosti:
Byl kontaktován jiný dodavatel, výrobce, CERT nebo koordinátor?	☐ Ne ☐ Ano ☐ Neznámé Pokud ano, uveďte subjekt, ID případu a datum:
Plánujete po nápravě problém projednat nebo zveřejnit?	☐ Ne ☐ Ano ☐ Neznámé Pokud ano, uveďte podrobnosti:
Preferované datum koordinovaného zveřejnění, pokud existuje	

Poznámka ke koordinovanému zveřejnění:

Neveřejné informace o zranitelnosti uchovávejte v důvěrnosti až do dohodnutého data zveřejnění. Pokud se úroveň rizika změní, bude zaznamenáno aktivní zneužívání nebo se veřejné zveřejnění stane pravděpodobným, neprodleně kontaktujte security@saluscontrols.com, aby bylo možné plán zveřejnění znovu posoudit.

7. Navrhovaná náprava nebo zmírnění rizika (volitelné)

- Navrhované odstranění hlavní příčiny, je-li známo: _____
- Navrhované dočasné zmírnění rizika nebo náhradní řešení, je-li známo: _____
- Relevantní oborová praxe, obranné pravidlo nebo reference: _____

8. Preference pro uvedení poděkování

Volba	Odpověď
Můžeme vás veřejně uvést v poděkování, pokud bude zveřejněno bezpečnostní upozornění?	☐ Ano ☐ Ne
Zobrazované jméno, alias nebo organizace	
Preferovaný odkaz na profil nebo referenci, pokud to zásady umožňují	

9. Přílohy a doplňující informace

Uvedte prosím všechny soubory přiložené k hlášení. Neuvádějte hesla, autentizační tokeny, soukromé klíče ani zbytečné osobní údaje či údaje zákazníků.

Pole	Odpověď
Jsou k tomuto hlášení přiloženy soubory?	☐ Ano ☐ Ne
Typ přiložených souborů	☐ Snímky obrazovky ☐ Protokoly ☐ Video ☐ Proof of concept ☐ Záznam síťového provozu ☐ Jiné
Popis přiložených souborů	
Další informace relevantní k hlášení	
Požadavky na důvěrnost nebo nakládání s informacemi	

Pokud přikládáte protokoly, snímky obrazovky, videa, záznamy síťového provozu nebo materiály proof of concept, odstraňte před odesláním hlášení zbytečné osobní údaje, údaje zákazníků, hesla, autentizační tokeny, soukromé klíče a další citlivé informace.

10. Potvrzení jednání v dobré víře

Odesláním tohoto hlášení oznamovatel podle svého nejlepšího vědomí potvrzuje, že:

- ☐ Hlášení je přesné a informace byly získány v rámci bezpečnostního výzkumu prováděného v dobré víře.
- ☐ Testování bylo omezeno na systémy, zařízení, účty a data, které oznamovatel vlastní nebo k jejichž testování byl oprávněn.
- ☐ Bylo zabráněno zbytečnému přístupu k neveřejným údajům, jejich uchovávání nebo zveřejnění.
- ☐ Oznamovatel bude koordinovat zveřejnění v souladu se zveřejněnými zásadami, s ohledem na platné právní předpisy a případnou naléhavou změnu rizika pro uživatele.
- ☐ Potvrzuji, že jsem úmyslně neuvedl(a) hesla, autentizační tokeny, soukromé klíče ani zbytečné osobní údaje či údaje zákazníků.

Datum odeslání: _____

Jméno nebo alias oznamovatele, pokud je uveden:

Jak toto hlášení odeslat

Vyplněný formulář zašlete e-mailem na adresu: security@saluscontrols.com

Podezření na zranitelnost můžete nahlásit také přímo e-mailem bez použití tohoto formuláře. Použití formuláře doporučujeme, protože společnosti SALUS Controls PLC pomáhá efektivně shromáždit informace potřebné k posouzení hlášení.