

Zásady pro zveřejňování zranitelností

Odpovědné hlášení, vyšetřování a náprava bezpečnostních zranitelností

Verze	Datum účinnosti	Vlastník dokumentu	Kontakt
1.0	Září 2026	Bezpečnostní tým společnosti SALUS Controls PLC	security@saluscontrols.com

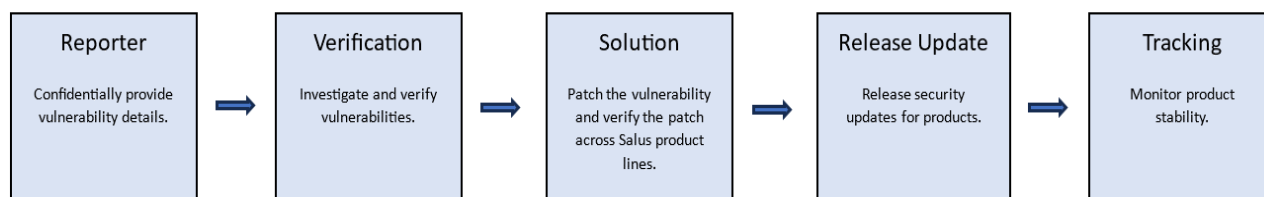
1. Úvod	2
2. Rozsah	2
3. Nahlášení zranitelnosti	3
4. Informace, které je třeba uvést.....	3
5. Proces reakce	4
6. Náprava na základě rizika.....	4
7. Koordinované zveřejnění zranitelnosti.....	4
8. Podpora bezpečnostních aktualizací	5
9. Mimo rozsah	5
10. Odpovědný bezpečnostní výzkum	5
11. Kontakt.....	6
12. Aktualizace zásad.....	6
13. Poděkování.....	6

1. Úvod

SALUS Controls PLC je odhodlána chránit bezpečnost svých produktů, služeb a zákazníků. Víťame odpovědná hlášení od zákazníků, bezpečnostních výzkumníků, partnerů, vývojářů a dalších členů bezpečnostní komunity, kteří identifikují potenciální bezpečnostní zranitelnosti týkající se produktů nebo služeb společnosti SALUS Controls PLC.

Naším cílem je neprodleně prošetřit potenciální hlášení zranitelností, po celou dobu procesu vhodně komunikovat s nahlášující stranou a poskytnout přiměřenou nápravu nebo zmírnění k ochraně uživatelů.

Potenciální bezpečnostní zranitelnosti nahláste soukromě na adresu security@saluscontrols.com. Společnost SALUS Controls PLC potvrdí přijetí do tří pracovních dnů, v každém případě nejpozději do sedmi kalendářních dnů. Toto potvrzení pouze potvrzuje přijetí informace a neznamena, že nahlášený problém byl potvrzen jako zranitelnost.



2. Rozsah

Tyto zásady se vztahují na bezpečnostní zranitelnosti týkající se:

- Produktů společnosti SALUS Controls PLC
- Firmwaru a softwaru
- Mobilních aplikací
- Cloudových služeb
- Veřejně přístupných webových aplikací a webových stránek

V případě dotazů týkajících se instalace produktu, konfigurace, záruky nebo jiných záležitostí nesouvisejících s bezpečností se prosím obraťte na náš tým zákaznické podpory prostřednictvím standardních podpůrných kanálů.

Přijímáme bezpečnostní hlášení týkající se produktů SALUS bez ohledu na fázi jejich životního cyklu. U produktů v rámci zveřejněného období bezpečnostní podpory jsou zranitelnosti a bezpečnostní aktualizace řešeny v souladu s příslušnými právními povinnostmi. U produktů mimo toto období společnost SALUS Controls PLC hlášení i nadále posoudí a může poskytnout zmírňující opatření, doporučení k migraci nebo jiné pokyny podle rizika, technické proveditelnosti a příslušných povinností.

3. Nahlášení zranitelnosti

Pokud se domníváte, že jste identifikovali bezpečnostní zranitelnost, nahlase ji prosím soukromě e-mailem na adresu security@saluscontrols.com.

Hlášení lze podávat anonymně. Absence jména nebo obousměrného kontaktního způsobu nezabrání přijetí ani počátečnímu posouzení hlášení, může však omezit naši schopnost vyžádat si další informace, poskytovat aktualizace stavu nebo nabídnout veřejné uznání.

Přijímáme počáteční hlášení zaslané běžným e-mailem nebo jiným kanálem. Pokud je třeba vyměnit exploit kód, přihlašovací údaje, osobní údaje, konfigurace zákazníků nebo jiné citlivé informace, společnost SALUS Controls PLC nabídne dostupnou zabezpečenou metodu pro další komunikaci. Neschopnost nebo rozhodnutí nahlašující strany nepoužít šifrování samo o sobě nepovede k odmítnutí hlášení.

4. Informace, které je třeba uvést

Abyste nám pomohli hlášení efektivně prošetřit, uveďte prosím pokud možno následující:

- Název a model produktu
- Verzi firmwaru nebo softwaru
- Popis zranitelnosti
- Kroky potřebné k reprodukci problému
- Očekávané a skutečné chování
- Potenciální bezpečnostní dopad
- Snímky obrazovky, protokoly nebo proof-of-concept, jsou-li k dispozici
- Vaše preferované kontaktní údaje pro další komunikaci

Nezahrnujte prosím citlivé osobní údaje, pokud to není nezbytné k prokázání zranitelnosti.

Uveďte prosím také, pokud je to známo, zda je problém veřejně známý, zda je aktivně zneužíván, zda ovlivnil uživatele nebo zda byl nahlášen jinému dodavateli, výrobcí či koordinátorovi. Pro přijetí a zaregistrování hlášení není nutné uvést všechny požadované údaje.

Během koordinovaného zveřejňování je přístup k neveřejným informacím o zranitelnosti omezen na základě potřeby znát danou informaci. Společnost SALUS Controls PLC může nezbytné informace sdílet s produktovými týmy, dodavateli, koordinátory, dotčenými stranami nebo příslušnými orgány za účelem ověření, nápravy, ochrany uživatelů a dodržení právních povinností, a to s odpovídajícími kontrolami důvěrnosti a ochrany osobních údajů.

Osobní údaje předložené spolu s hlášením zranitelnosti jsou zpracovávány v souladu s příslušným oznámením o ochraně osobních údajů společnosti SALUS Controls PLC. Více informací naleznete v oznámení o ochraně osobních údajů na adrese: <https://saluscontrols.com/cz/ochrana-osobnich-udaju-a-soubory-cookie/>.

5. Proces reakce

Po obdržení vašeho hlášení společnost SALUS Controls PLC:

- Potvrdí přijetí do tří pracovních dnů, v každém případě nejpozději do sedmi kalendářních dnů; pokud je to možné, uvede jedinečný identifikátor případu a předběžné informace o stavu.
- Provede počáteční posouzení do sedmi pracovních dnů
- Ověří nahlášenou zranitelnost
- Posoudí její závažnost a potenciální dopad
- Vypracuje plán nápravy nebo bezpečnostní aktualizaci, je-li to vhodné
- Bude vás informovat po celou dobu vyšetřování a nápravy
- Dokud je případ aktivní, poskytne věcnou aktualizaci stavu alespoň jednou za 30 kalendářních dnů a bude komunikovat dříve, pokud dojde k podstatné změně potvrzeného rozsahu, rizika, přístupu k nápravě nebo data zveřejnění.
- Pokud jsou potřeba další informace, můžeme vás během vyšetřování kontaktovat.

6. Náprava na základě rizika

Potvrzené zranitelnosti jsou prioritizovány podle technické závažnosti, zneužitelnosti, dotčených produktů, potenciálního dopadu, expozice uživatelů, důkazů o aktivním zneužívání, dostupných zmírňujících opatření a potřeb bezpečného nasazení. Číselné skóre může posouzení informovat, ale samo o sobě neurčuje prioritu nápravy.

Společnost SALUS Controls PLC stanoví cíl nápravy specifický pro daný případ a sděluje nahlašující straně podstatné změny. Pokud okamžitá náprava není možná, může být před dostupností trvalého řešení poskytnuto vhodné zmírňující opatření nebo pokyny ke snížení rizika.

7. Koordinované zveřejnění zranitelnosti

Společnost SALUS Controls PLC spolupracuje s nahlašující stranou a v případě potřeby s dodavateli, koordinátory a dalšími dotčenými stranami na stanovení data zveřejnění specifického pro daný případ. Termín může být upraven podle závažnosti, aktivního zneužívání, rizika pro uživatele, pokroku v nápravě a nasazení, závislosti v dodavatelském řetězci a příslušných právních či regulačních povinností. Podstatné změny cílového data budou sděleny příslušným stranám.

Společnost SALUS Controls PLC může urychlit oznámení uživatelům nebo veřejné zveřejnění, pokud je zranitelnost již veřejně známá, je aktivně zneužívána, představuje naléhavé riziko pro uživatele, hrozí její únik, nebo pokud to vyžaduje zákon. Pokud kompletní oprava ještě není k dispozici, může SALUS poskytnout dočasné zmírňující opatření nebo pokyny ke snížení rizika, aniž by zbytečně usnadňovala zneužití.

Informace o odstraněných zranitelnostech budou zveřejněny ve srozumitelných bezpečnostních doporučeních. Doporučení budou identifikovat zranitelnost a dotčené produkty, data zveřejnění a revize, potenciální dopad a závažnost, dostupnou nápravu nebo zmírnění, požadované kroky uživatelů a kontaktní informace. Doporučení týkající se komponent třetích stran mohou odkazovat na autoritativní informace od dodavatele, pokud to uživatelům umožní zjistit, zda jsou produkty SALUS dotčeny.

Informace o zranitelnosti budou rovněž zpřístupněny ve všeobecně uznávaném strojově čitelném formátu, pokud nebude zdůvodnění pro neučinění tak zdokumentováno a schváleno. Zveřejnění může být odloženo nebo vynecháno pouze tehdy, pokud byly příslušné podmínky posouzeny, zdokumentovány a schváleny.

Pokud to vyžaduje platný zákon nebo je to nezbytné k ochraně uživatelů, společnost SALUS Controls PLC informuje dotčené uživatele a poskytne dostupná zmírňující nebo nápravná doporučení prostřednictvím vhodných přístupných kanálů.

8. Podpora bezpečnostních aktualizací

Společnost SALUS Controls PLC poskytuje bezpečnostní aktualizace po celou dobu podpory stanovenou pro každý příslušný produkt. Doba podpory je určena v souladu s příslušnými právními požadavky s ohledem na očekávanou dobu používání produktu, jeho povahu a přiměřená očekávání uživatelů.

Doba podpory bude činit nejméně pět let, pokud se neočekává, že produkt bude používán po kratší dobu, a může být delší, je-li to odůvodněno očekávanou životností produktu. Příslušné datum ukončení doby podpory bude sděleno prostřednictvím relevantních informací o produktu.

9. Mimo rozsah

Všechna potenciální bezpečnostní hlášení jsou zaregistrována a projdou počátečním posouzením. Problémy, které jsou čistě funkční, komerční nebo související s podporou, mohou být přesměrovány na příslušný podpůrný kanál. Pokud problém nelze zprvu reprodukovat, společnost SALUS Controls PLC může požádat o další informace a hlášení znovu posoudit, jakmile budou k dispozici nové důkazy.

Teoretické problémy, scénáře vyžadující fyzický přístup, podmínky odepření služby, scénáře sociálního inženýrství a závislosti na třetích stranách jsou posuzovány podle jejich reálného bezpečnostního dopadu, zneužitelnosti a zamýšleného i přiměřeně předvídatelného použití produktu.

Zranitelnosti v komponentách třetích stran integrovaných do produktu SALUS, dodávaných s ním nebo na nich závislých, nadále podléhají posouzení dopadu na produkt SALUS.

10. Odpovědný bezpečnostní výzkum

Společnost SALUS Controls PLC podporuje odpovědný bezpečnostní výzkum prováděný v dobré víře. Žádáme výzkumníky, aby:

- Jednali odpovědně a eticky
- Nenarušovali produkty, služby ani provoz zákazníků
- Nepřistupovali k datům zákazníků, neupravovali je ani je nemazali
- Nahlašovali zranitelnosti soukromě prostřednictvím postupu popsánoho v těchto zásadách
- Poskytli společnosti SALUS Controls PLC přiměřený čas na vyšetření a nápravu problému před veřejným zveřejněním

- Dodržovali všechny platné zákony a předpisy při provádění bezpečnostního výzkumu

Pokud nahlašující strana jedná v dobré víře, dodržuje tyto zásady, vyhýbá se způsobení újmy a hlásí problémy včas, společnost SALUS Controls PLC nemá v úmyslu podniknout právní kroky výhradně z důvodu bezpečnostního výzkumu prováděného v souladu s těmito zásadami. Toto prohlášení neopravňuje k přístupu k systémům nebo datům třetích stran, nezavazuje třetí stranu ani orgán a nezbavuje nahlašující stranu povinnosti dodržovat platné právo a získat požadované povolení.

11. Kontakt

V případě jakýchkoli bezpečnostních hlášení nebo dotazů týkajících se těchto zásad nás kontaktujte:

Bezpečnostní tým společnosti SALUS Controls PLC

E-mail: security@saluscontrols.com

12. Aktualizace zásad

Tyto zásady jsou přezkoumávány nejméně jednou ročně a po podstatných změnách platných právních požadavků, komunikačních kanálů, rozsahu produktů nebo procesů řešení zranitelností. Aktuální verze, datum zveřejnění, datum poslední aktualizace a vlastník zásad jsou uvedeny u zveřejněných zásad.

13. Poděkování

Se souhlasem nahlašující strany může společnost SALUS Controls PLC uvést jméno, alias nebo organizaci nahlašující strany, která předloží platné hlášení zranitelnosti a podpoří koordinované zveřejnění. Hlášení lze podávat anonymně a odmítnutí uznání nemá vliv na přijetí, prioritizaci ani rozhodnutí o nápravě.

Tyto zásady nezakládají program bug bounty ani nezaručují finanční či jiné odměny.