

SALUS Controls PLC - Pranešimo apie įtariamą saugumo pažeidžiamumą forma

Naudokite šią formą pranešti apie įtariamą saugumo pažeidžiamumą, susijusį su SALUS produktu, programa, debesijos paslauga ar svetaine.

Pateikite kuo daugiau turimos informacijos. Kad galėtume priimti jūsų pranešimą, nebūtina užpildyti visų laukų.

Pranešimą galite pateikti anonimiškai. Tačiau, jei nepateiksite kontaktinių duomenų, galime neturėti galimybės paprašyti papildomos informacijos ar informuoti jus apie pranešimo nagrinėjimo eigą.

Užpildytą formą siųskite adresu security@saluscontrols.com.

Neįtraukite slaptažodžių, autentifikavimo žetonų, privačių raktų ar nereikalingų asmens / klientų duomenų.

Laukai, pažymėti „Privaloma“, yra privalomi tik tada, kai atitinkama informacija pagrįstai prieinama. Net jei neturite visos informacijos, pranešimą vis tiek galite pateikti.

Pranešimas apie įtariamą saugumo pažeidžiamumą

1. Pranešėjo informacija

Laukas	Atsakymas
Vardas arba slapyvardis (neprivaloma)	
Organizacija (neprivaloma)	
El. paštas / kontaktavimo būdas (privaloma, nebent pranešama anonimiškai)	
Pageidaujama kalba (neprivaloma)	
Ar pranešate anonimiškai?	☐ Taip ☐ Ne

2. Paveiktas produktas arba komponentas

Laukas	Atsakymas
Produkto arba paslaugos pavadinimas (privaloma)	
Modelis (jei taikoma)	
Aparatinės įrangos versija (jei žinoma)	
Programinės aparatinės įrangos / programinės įrangos / programos versija (jei žinoma)	

Laukas	Atsakymas
Šalis / regionas	
Kita svarbi konfigūracijos informacija	

3. Įtariamo saugumo pažeidžiamumo aprašymas

Laukas	Atsakymas
Trumpas pavadinimas (privaloma)	
Aprašykite nustatytą saugumo problemą (privaloma)	
Kada pirmą kartą pastebėjote problemą?	
Ko tikėjotės?	
Kas iš tikrųjų įvyko?	
Ar galite atkurti problemą?	☐ Taip ☐ Ne ☐ Kartais ☐ Nežinoma
Jei įmanoma, aprašykite veiksmus, reikalingus problemai atkurti:	
Kokių poveikį saugumui, jūsų nuomone, gali turėti ši problema?	
Ar pridėta priedų? Galite pridėti susijusias ekrano kopijas, žurnalus, vaizdo įrašus ar koncepcijos įrodymo informaciją.	☐ Taip ☐ Ne

Papildoma techninė informacija (neprivaloma – saugumo tyrėjams)

Laukas	Atsakymas
Pažeidžiamumo tipas (autentifikavimo apėjimas, injekcija, atminties pažeidimas ir kt.), jei žinomas	
CWE / CVE, jei žinoma	
Techninė priežastis / išsami informacija	
Testavimo aplinka / konfigūracija	
Koncepcijos įrodymas	

4. Atakos scenarijus

Atakos scenarijus skiriasi nuo problemos atkūrimo procedūros. Aprašykite, kaip realus užpuolikas galėtų išnaudoti šį pažeidžiamumą.

Laukas	Atsakymas
Jei žinoma, aprašykite, kaip kas nors galėtų išnaudoti šį pažeidžiamumą	
Užpuoliko prieiga	☐ Nuotolinis tinklas ☐ Gretimas tinklas ☐ Local network ☐ Local device ☐ Physical access ☐ Nežinoma
Reikalinga naudotojo sąveika	☐ Taip ☐ Ne ☐ Nežinoma
Reikalingi specialūs leidimai / paskyra	☐ Taip ☐ Ne ☐ Nežinoma Jei taip, aprašykite reikalingus leidimus / paskyrą:

5. Poveikio vertinimas (neprivaloma)

Užpildykite šį skyrių, jei galite įvertinti galimą poveikį.

Poveikio sritis	Pranešėjo vertinimas
Konfidencialumas	☐ Nene ☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Nežinoma
Vientisumas	☐ Nene ☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Nežinoma
Prieinamumas	☐ Nene ☐ Žemas ☒ Vidutinis ☐ Aukštas ☐ Nežinoma
Sauga	☐ Nene ☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Nežinoma
Privatumas	☐ Nene ☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Nežinoma
Poveikis tiekimo grandinei arba platesnei ekosistemai	☐ Nėra ☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Nežinoma
Siūlomas kritiškumo lygis, jei žinomas (neprivaloma)	☐ Žemas ☐ Vidutinis ☐ Aukštas ☐ Kritinis ☐ Nežinoma
CVSS vektorius, jei žinomas (neprivaloma)	

6. Išnaudojimo ir atskleidimo būseną

Laukas	Atsakymas
Ar pažeidžiamumas jau viešai paskelbtas?	☐ Ne ☐ Taip ☐ Nežinoma Jei taip, nurodykite URL ir datą:
Ar koncepcijos įrodymas yra viešai prieinamas?	☐ Ne ☐ Taip ☐ Nežinoma Jei taip, nurodykite URL ir datą:
Ar žinoma arba įtariama, kad pažeidžiamumas aktyviai išnaudojamas?	☐ Ne ☐ Taip ☐ Nežinoma Jei taip, pateikite išsamią informaciją:
Ar buvo susisiekiama su kitu gamintoju, tiekėju, CERT ar koordinatoriumi?	☐ Ne ☐ Yes ☐ Nežinoma Jei taip, nurodykite šalį, bylos ID ir datą:
Ar planuojate aptarti arba paskelbti problemą po jos ištaisymo?	☐ Ne ☐ Taip ☐ Nežinoma Jei taip, pateikite išsamią informaciją:
Pageidaujama koordinuoto atskleidimo data, jei taikoma	

Pastaba dėl koordinuoto atskleidimo:

Neviešą informaciją apie pažeidžiamumą laikykite konfidencialia iki sutartos atskleidimo datos. Jei rizika pasikeičia, pastebimas aktyvus išnaudojimas arba tampa tikėtinas viešas atskleidimas, nedelsdami susisiekite adresu security@saluscontrols.com, kad būtų galima iš naujo įvertinti atskleidimo planą. security@saluscontrols.com

7. Siūlomas ištaisymas arba rizikos mažinimas (neprivaloma)

- Siūlomas pagrindinės priežasties ištaisymas, jei žinomas: _____
- Siūloma laikina rizikos mažinimo priemonė arba alternatyvus sprendimas, jei žinomas: _____
- Atitinkama pramonės praktika, apsaugos taisyklė arba nuoroda: _____

8. Pageidavimas dėl viešo paminėjimo

Pasirinkimas	Atsakymas
Ar galime jus viešai paminėti, jei bus paskelbtas saugumo pranešimas?	☐ Taip ☐ Ne
Viešai rodomas vardas, slapyvardis arba organizacija	
Pageidaujama profilio arba nuorodos nuoroda, jei tai leidžiama pagal politiką	

9. Priedai ir papildoma informacija

Nurodykite visus prie pranešimo pridėtus failus. Neįtraukite slaptažodžių, autentifikavimo žetonų, privačių raktų ar nereikalingų asmens / klientų duomenų.

Laukas	Atsakymas
Ar prie šio pranešimo pridėti failai?	☐ Taip ☐ Ne
Pridėtų failų tipas	☐ Ekrano kopijos ☐ Žurnalai ☐ Vaizdo įrašas ☐ Konceptijos įrodymas ☐ Paketų fiksavimas ☐ Kita
Pridėtų failų aprašymas	
Papildoma su pranešimu susijusi informacija	
Konfidencialumo arba tvarkymo reikalavimai	

Jei pridedate žurnalus, ekrano kopijas, vaizdo įrašus, paketų fiksavimo duomenis ar koncepcijos įrodymo medžiagą, prieš pateikdami pranešimą pašalinkite nereikalingus asmens duomenis, klientų duomenis, slaptažodžius, autentifikavimo žetonus, privačius raktus ar kitą neskelbtiną informaciją.

10. Sąžiningo veikimo patvirtinimas

Pateikdamas šį pranešimą, pranešėjas, kiek jam žinoma, patvirtina, kad:

- ☐ Pranešimas yra tikslus ir parengtas vykdant sąžiningus saugumo tyrimus.
- ☐ Testavimas apsiribojo sistemomis, įrenginiais, paskyromis ir duomenimis, kurie priklauso pranešėjui arba kuriuos jis turėjo leidimą testuoti.
- ☐ Buvo vengiama nereikalingos prieigos prie neviešų duomenų, jų saugojimo ar atskleidimo.
- ☐ Pranešėjas koordinuos atskleidimą pagal paskelbtą politiką, laikydamasis taikomų teisės aktų ir atsižvelgdamas į bet kokių skubų naudotojų rizikos pasikeitimą.
- ☐ Patvirtinu, kad sąmoningai neįtraukiau slaptažodžių, autentifikavimo žetonų, privačių raktų ar nereikalingų asmens / klientų duomenų.

Pateikimo data: _____

Pranešėjo vardas arba slapyvardis, jei nurodytas:

Kaip pateikti šį pranešimą

Užpildytą formą siųskite el. paštu: security@saluscontrols.com

Apie įtariamą saugumo pažeidžiamumą taip pat galite pranešti tiesiogiai el. paštu, nenaudodami šios formos. Rekomenduojame naudoti šią formą, nes ji padeda SALUS Controls PLC surinkti informaciją, reikalingą veiksmingai įvertinti pranešimą.