

SALUS Controls PLC - Formulier voor melding van een vermoedelijke kwetsbaarheid

Gebruik dit formulier om een vermoedelijke beveiligingskwetsbaarheid te melden die betrekking heeft op een SALUS-product, applicatie, clouddienst of website.

Vul zoveel mogelijk informatie in. U hoeft niet elk veld in te vullen om uw melding te kunnen indienen. U kunt een melding anoniem indienen. Als u geen contactgegevens verstrekt, kunnen wij mogelijk geen aanvullende informatie opvragen of u op de hoogte houden van uw melding.

Stuur het ingevulde formulier naar security@saluscontrols.com.

Neem geen wachtwoorden, authenticatietokens, privésleutels of onnodige persoonsgegevens/klantgegevens op.

Velden met de aanduiding 'Verplicht' zijn alleen verplicht voor zover de informatie redelijkerwijs beschikbaar is. Ook als u niet over alle informatie beschikt, kunt u de melding indienen.

Melding van een vermoedelijke kwetsbaarheid

1. Gegevens van de melder

Veld	Antwoord
Naam of alias (optioneel)	
Organisatie (optioneel)	
E-mail/contactmethode (verplicht, tenzij u anoniem meldt)	
Voorkeurstaal (optioneel)	
Anoniem melden?	☐ Ja ☐ Nee

2. Betrokken product of onderdeel

Veld	Antwoord
Naam van product of dienst (verplicht)	
Model (indien van toepassing)	
Hardwareversie (indien bekend)	
Firmware-/software-/applicatieversie (indien bekend)	
Land/regio	

Veld	Antwoord
Overige relevante configuratiegegevens	

3. Beschrijving van de vermoedelijke kwetsbaarheid

Veld	Antwoord
Korte titel (verplicht)	
Beschrijf het beveiligingsprobleem dat u hebt vastgesteld (verplicht)	
Wanneer hebt u het probleem voor het eerst opgemerkt?	
Wat verwachtte u dat er zou gebeuren?	
Wat gebeurde er daadwerkelijk?	
Kunt u het probleem reproduceren?	☐ Ja ☐ Nee ☐ Soms ☐ Onbekend
Beschrijf indien mogelijk de stappen die nodig zijn om het probleem te reproduceren:	
Welke gevolgen voor de beveiliging kan het probleem volgens u hebben?	
Bijlagen toegevoegd? U kunt relevante screenshots, logbestanden, video's of proof-of-concept-informatie toevoegen.	☐ Ja ☐ Nee

Aanvullende technische informatie (optioneel – voor beveiligingsonderzoekers)

Veld	Antwoord
Type kwetsbaarheid (omzeiling van authenticatie, injectie, geheugenbeschadiging enz.), indien bekend	
CWE/CVE, indien bekend	
Technische oorzaak/details	
Testomgeving/configuratie	
Proof of concept	

4. Aanvalsscenario

Het aanvalsscenario verschilt van de procedure om het probleem te reproduceren. Beschrijf hoe een realistische aanvaller misbruik zou kunnen maken van het probleem.

Veld	Antwoord
Beschrijf, indien bekend, hoe iemand misbruik zou kunnen maken van deze kwetsbaarheid	
Toegang van de aanvaller	☐ Remote network ☐ Adjacent network ☐ Local network ☐ Local device ☐ Physical access ☐ Onbekend
Gebruikersinteractie vereist	☐ Ja ☐ Nee ☐ Onbekend
Speciale machtigingen/account vereist	☐ Ja ☐ Nee ☐ Onbekend Zo ja, beschrijf de vereiste machtigingen/het vereiste account:

5. Impactbeoordeling (optioneel)

Vul dit gedeelte in als u de mogelijke impact kunt beoordelen.

Impactgebied	Beoordeling door de melder
Vertrouwelijkheid	☐ Neene ☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Onbekend
Integriteit	☐ Neene ☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Onbekend
Beschikbaarheid	☐ Neene ☐ Laag ☒ Gemiddeld ☐ Hoog ☐ Onbekend
Veiligheid	☐ Neene ☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Onbekend
Privacy	☐ Neene ☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Onbekend
Impact op de toeleveringsketen of het bredere ecosysteem	☐ Geen ☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Onbekend
Voorgestelde ernst, indien beschikbaar (optioneel)	☐ Laag ☐ Gemiddeld ☐ Hoog ☐ Kritiek ☐ Onbekend
CVSS-vector, indien beschikbaar (optioneel)	

6. Status van misbruik en openbaarmaking

Veld	Antwoord
Is de kwetsbaarheid al openbaar?	☐ Nee ☐ Ja ☐ Onbekend Zo ja, vermeld de URL en datum:
Is er een openbare proof of concept?	☐ Nee ☐ Ja ☐ Onbekend Zo ja, vermeld de URL en datum:
Is actief misbruik bekend of wordt dit vermoed?	☐ Nee ☐ Ja ☐ Onbekend Zo ja, geef details:
Is er contact opgenomen met een andere leverancier, toeleverancier, CERT of coördinator?	☐ Nee ☐ Yes ☐ Onbekend If yes, please provide party, case ID and date:
Bent u van plan het probleem na herstel te bespreken of te publiceren?	☐ Nee ☐ Ja ☐ Onbekend Zo ja, geef details:
Gewenste datum voor gecoördineerde openbaarmaking, indien van toepassing	

Opmerking over gecoördineerde openbaarmaking:

Houd niet-openbare informatie over de kwetsbaarheid vertrouwelijk tot de overeengekomen openbaarmakingsdatum. Als het risico verandert, actief misbruik wordt waargenomen of openbare bekendmaking waarschijnlijk wordt, neem dan zo snel mogelijk contact op via security@saluscontrols.com, zodat het openbaarmakingsplan opnieuw kan worden beoordeeld. security@saluscontrols.com

7. Voorgestelde oplossing of risicobeperking (optioneel)

- Suggested root-cause fix, if known: _____
- Suggested temporary mitigation or workaround, if known: _____
- Relevant industry practice, defensive rule or reference: _____

8. Voorkeur voor naamsvermelding

Keuze	Antwoord
Mogen wij u publiekelijk vermelden als er een beveiligingsadvies wordt gepubliceerd?	☐ Ja ☐ Nee
Weergavenaam, alias of organisatie	
Voorkeursprofiel of referentielink, indien toegestaan volgens het beleid	

9. Bijlagen en aanvullende informatie

Vermeld alle bestanden die u bij uw melding voegt. Neem geen wachtwoorden, authenticatietokens, privésleutels of onnodige persoonsgegevens/klantgegevens op.

Veld	Antwoord
Zijn er bestanden bij deze melding gevoegd?	☐ Ja ☐ Nee
Type of files attached	☐ Screenshots ☐ Logs ☐ Video ☐ Proof of concept ☐ Packet capture ☐ Other
Beschrijving van de bijgevoegde bestanden	
Aanvullende informatie die relevant is voor de melding	
Vereisten voor vertrouwelijkheid of behandeling	

Als u logbestanden, screenshots, video's, pakketopnamen of proof-of-concept-materiaal toevoegt, verwijder dan vóór indiening onnodige persoonsgegevens, klantgegevens, wachtwoorden, authenticatietokens, privésleutels of andere gevoelige informatie.

10. Verklaring van handelen te goeder trouw

Door deze melding in te dienen, bevestigt de melder naar beste weten dat:

- ☐ De melding is juist en is verkregen door beveiligingsonderzoek te goeder trouw.
- ☐ Testing was limited to systems, devices, accounts and data the reporting party owns or was authorised to test.
- ☐ Onnodige toegang tot, bewaring van of openbaarmaking van niet-openbare gegevens is vermeden.
- ☐ De melder zal de openbaarmaking coördineren overeenkomstig het gepubliceerde beleid, met inachtneming van de toepasselijke wetgeving en eventuele dringende wijzigingen in het risico voor gebruikers.
- ☐ Ik bevestig dat ik niet opzettelijk wachtwoorden, authenticatietokens, privésleutels of onnodige persoonsgegevens/klantgegevens heb opgenomen.

Datum van indiening: _____

Naam of alias van de melder, indien opgegeven:

Zo dient u deze melding in

Stuur het ingevulde formulier per e-mail naar: security@saluscontrols.com

U kunt een vermoedelijke kwetsbaarheid ook rechtstreeks per e-mail melden zonder dit formulier te gebruiken. Het gebruik van dit formulier wordt aanbevolen, omdat SALUS Controls PLC hiermee de informatie kan verzamelen die nodig is om de melding efficiënt te beoordelen.