

SALUS Controls PLC - Formular til indberetning af formodet sikkerhedssårbarhed

Brug denne formular til at indberette en formodet sikkerhedssårbarhed, der påvirker et SALUS-produkt, en applikation, en cloudtjeneste eller et websted.

Udfyld så mange oplysninger som muligt. Du behøver ikke udfylde alle felter, for at vi kan modtage din indberetning.

Du kan indsende en indberetning anonymt. Hvis du ikke angiver kontaktoplysninger, kan vi dog muligvis ikke bede om yderligere oplysninger eller give dig opdateringer om din indberetning.

Når formularen er udfyldt, bedes du sende den til security@saluscontrols.com.

Medtag ikke adgangskoder, godkendelsestokens, private nøgler eller unødvendige person- eller kundedata.

Felter markeret med "Påkrævet" skal kun udfyldes, hvis oplysningerne med rimelighed er tilgængelige.

Du kan stadig indsende indberetningen, selv om du ikke har alle oplysninger.

Indberetning af formodet sikkerhedssårbarhed

1. Oplysninger om indberetteren

Felt	Svar
Navn eller alias (valgfrit)	
Organisation (valgfrit)	
E-mail/kontaktmetode (påkrævet, medmindre indberetningen er anonym)	
Foretrukket sprog (valgfrit)	
Indberetter du anonymt?	☐ Ja ☐ Nej

2. Berørt produkt eller komponent

Felt	Svar
Produkt- eller tjenestenavn (påkrævet)	
Model (hvis relevant)	
Hardwareversion (hvis kendt)	
Firmware-/software-/applikationsversion (hvis kendt)	
Land/region	

Felt	Svar
Andre relevante konfigurationsoplysninger	

3. Beskrivelse af den formodede sikkerhedssårbarhed

Felt	Svar
Kort titel (påkrævet)	
Beskriv det sikkerhedsproblem, du har identificeret (påkrævet)	
Hvornår bemærkede du problemet første gang?	
Hvad forventede du ville ske?	
Hvad skete der faktisk?	
Kan du reproducere problemet?	☐ Ja ☐ Nej ☐ Nogle gange ☐ Ukendt
Beskriv om muligt de trin, der er nødvendige for at reproducere problemet:	
Hvilke sikkerhedsmæssige konsekvenser mener du, at problemet kan have?	
Er der vedlagt bilag? Du kan vedlægge relevante skærbilleder, logfiler, videoer eller proof-of-concept-oplysninger.	☐ Ja ☐ Nej

Yderligere tekniske oplysninger (valgfrit – for sikkerhedsforskere)

Felt	Svar
Type af sårbarhed (omgåelse af godkendelse, injection, hukommelsesfejl osv.), hvis kendt	
CWE/CVE, hvis kendt	
Teknisk årsag / detaljer	
Testmiljø / konfiguration	
Proof of concept	

4. Angrebsscenarie

Angrebsscenariet er forskelligt fra fremgangsmåden til at reproducere problemet. Beskriv, hvordan en realistisk angriber vil kunne udnytte sårbarheden.

Felt	Svar
Beskriv, hvis det er kendt, hvordan nogen vil kunne udnytte denne sårbarhed	
Angriberens adgang	☐ Fjernnetværk ☐ Tilstødende netværk ☐ Local network ☐ Local device ☐ Physical access ☐ Ukendt
Kræves brugerinteraktion	☐ Ja ☐ Nej ☐ Ukendt
Kræves særlige rettigheder/konto	☐ Ja ☐ Nej ☐ Ukendt Hvis ja, beskriv de nødvendige rettigheder/den nødvendige konto:

5. Vurdering af konsekvenser (valgfrit)

Udfyld dette afsnit, hvis du kan vurdere de potentielle konsekvenser.

Konsekvensområde	Indberetterens vurdering
Fortrolighed	☐ Nejne ☐ Lav ☐ Middel ☐ Høj ☐ Ukendt
Integritet	☐ Nejne ☐ Lav ☐ Middel ☐ Høj ☐ Ukendt
Tilgængelighed	☐ Nejne ☐ Lav ☒ Middel ☐ Høj ☐ Ukendt
Sikkerhed	☐ Nejne ☐ Lav ☐ Middel ☐ Høj ☐ Ukendt
Privatliv	☐ Nejne ☐ Lav ☐ Middel ☐ Høj ☐ Ukendt
Konsekvenser for forsyningskæden eller det bredere økosystem	☐ Ingen ☐ Lav ☐ Middel ☐ Høj ☐ Ukendt
Foreslået alvorlighedsgrad, hvis tilgængelig (valgfrit)	☐ Lav ☐ Middel ☐ Høj ☐ Kritisk ☐ Ukendt
CVSS-vektor, hvis tilgængelig (valgfrit)	

6. Status for udnyttelse og offentliggørelse

Felt	Svar
Er sårbarheden allerede offentlig kendt?	☐ Nej ☐ Ja ☐ Ukendt Hvis ja, angiv URL og dato:
Er et proof of concept offentligt tilgængeligt?	☐ Nej ☐ Ja ☐ Ukendt Hvis ja, angiv URL og dato:
Er aktiv udnyttelse kendt eller mistænkt?	☐ Nej ☐ Ja ☐ Ukendt Hvis ja, angiv nærmere oplysninger:
Er en anden producent, leverandør, et CERT eller en koordinator blevet kontaktet?	☐ Nej ☐ Yes ☐ Ukendt Hvis ja, angiv part, sags-ID og dato:
Planlægger du at omtale eller offentliggøre problemet efter afhjælpning?	☐ Nej ☐ Ja ☐ Ukendt Hvis ja, angiv nærmere oplysninger:
Foretrukken dato for koordineret offentliggørelse, hvis relevant	

Bemærkning om koordineret offentliggørelse:

Hold ikke-offentlige oplysninger om sårbarheden fortrolige indtil en aftalt dato for offentliggørelse. Hvis risikoen ændrer sig, der observeres aktiv udnyttelse, eller offentliggørelse bliver sandsynlig, bedes du straks kontakte security@saluscontrols.com, så planen for offentliggørelse kan revurderes. security@saluscontrols.com

7. Foreslået afhjælpning eller risikoreduktion (valgfrit)

- Foreslået løsning på den grundlæggende årsag, hvis kendt: _____
- Foreslået midlertidig risikoreduktion eller workaround, hvis kendt: _____
- Relevant branchepraksis, beskyttelsesregel eller reference: _____

8. Præference for offentlig anerkendelse

Valg	Svar
Må vi offentligt anerkende dig, hvis der offentliggøres en sikkerhedsmeddelelse?	☐ Ja ☐ Nej
Navn, alias eller organisation, der skal vises	
Foretrukket profil- eller referencelink, hvis det accepteres i henhold til politikken	

9. Bilag og yderligere oplysninger

Angiv alle filer, der er vedlagt din indberetning. Medtag ikke adgangskoder, godkendelsestokens, private nøgler eller unødvendige person- eller kundedata.

Felt	Svar
Er der vedlagt filer til denne indberetning?	☐ Ja ☐ Nej
Type af vedlagte filer	☐ Skærbilleder ☐ Logfiler ☐ Video ☐ Proof of concept ☐ Pakkecapture ☐ Andet
Beskrivelse af vedlagte filer	
Yderligere oplysninger, der er relevante for indberetningen	
Krav til fortrolighed eller håndtering	

Hvis du vedlægger logfiler, skærbilleder, videoer, pakkecaptures eller proof-of-concept-materiale, skal du fjerne unødvendige persondata, kundedata, adgangskoder, godkendelsestokens, private nøgler eller andre følsomme oplysninger, før du indsender indberetningen.

10. Bekræftelse på redelig sikkerhedsforskning

Ved at indsende denne indberetning bekræfter indberetteren efter bedste overbevisning, at:

- ☐ Indberetningen er korrekt og er udarbejdet som led i redelig sikkerhedsforskning.
- ☐ Testningen var begrænset til systemer, enheder, konti og data, som indberetteren ejer eller havde tilladelse til at teste.
- ☐ Unødvendig adgang til, opbevaring af eller videregivelse af ikke-offentlige data blev undgået.
- ☐ Indberetteren vil koordinere offentliggørelsen i overensstemmelse med den offentliggjorte politik med forbehold for gældende lovgivning og eventuelle akutte ændringer i risikoen for brugerne.
- ☐ Jeg bekræfter, at jeg ikke bevidst har medtaget adgangskoder, godkendelsestokens, private nøgler eller unødvendige person- eller kundedata.

Indsendelsesdato: _____

Indberetterens navn eller alias, hvis angivet:

Sådan indsender du denne indberetning

Send den udfyldte formular pr. e-mail til: security@saluscontrols.com

Du kan også indberette en formodet sikkerhedssårbarhed direkte via e-mail uden at bruge denne formular. Vi anbefaler at bruge formularen, da den hjælper SALUS Controls PLC med at indsamle de oplysninger, der er nødvendige for at vurdere indberetningen effektivt.