Politik for offentliggørelse af sårbarheder

Ansvarlig rapportering, undersøgelse og afhjælpning af sikkerhedssårbarheder

Version	Ikrafttrædelsesdato	Dokumentansvarlig	Kontakt
1.0	September 2026	SALUS Controls PLC Sikkerhedsteam	security@saluscontrols.com

1. Introduktion

SALUS Controls PLC er forpligtet til at beskytte sikkerheden i sine produkter, tjenester og for sine kunder. Vi modtager gerne ansvarlige rapporter fra kunder, sikkerhedsforskere, partnere, udviklere og andre medlemmer af sikkerhedsfællesskabet, som identificerer potentielle sikkerhedssårbarheder, der påvirker SALUS Controls PLCs produkter eller tjenester.

Vores mål er hurtigt at undersøge rapporter om potentielle sårbarheder, kommunikere passende med den rapporterende part gennem hele processen og iværksætte forholdsmæssig afhjælpning eller risikoreduktion for at beskytte brugerne.

Rapportér potentielle sikkerhedssårbarheder fortroligt til **security@saluscontrols.com**. SALUS Controls PLC bekræfter modtagelsen inden for tre arbejdsdage og under alle omstændigheder senest inden for syv kalenderdage. Denne bekræftelse bekræfter kun modtagelsen af oplysningerne og betyder ikke, at det rapporterede forhold er blevet bekræftet som en sårbarhed.

2. Omfang

Denne politik gælder for sikkerhedssårbarheder, der påvirker:

- SALUS Controls PLC-produkter
- Firmware og software
- Mobilapplikationer
- Cloudtjenester
- Offentligt tilgængelige webapplikationer og websteder

Ved spørgsmål om produktinstallation, konfiguration, garanti eller andre forhold, der ikke vedrører sikkerhed, bedes du kontakte vores kundesupport via de sædvanlige supportkanaler.

Vi modtager sikkerhedsrapporter om SALUS-produkter uanset deres livscyklusstatus. For produkter inden for den offentliggjorte sikkerhedssupportperiode håndteres sårbarheder og sikkerhedsopdateringer i overensstemmelse med gældende retlige forpligtelser. For produkter uden for denne periode vil SALUS Controls PLC fortsat vurdere rapporter og kan tilbyde risikoreducerende tiltag, vejledning om migrering eller anden rådgivning afhængigt af risiko, teknisk gennemførlighed og gældende forpligtelser.

3. Rapportering af en sårbarhed

Hvis du mener, at du har identificeret en sikkerhedssårbarhed, bedes du rapportere den fortroligt ved at sende en e-mail til **security@saluscontrols.com**.

Rapporter kan indsendes anonymt. Manglende navn eller mulighed for tovejskommunikation forhindrer ikke modtagelse eller indledende vurdering, men kan begrænse vores mulighed for at anmode om yderligere oplysninger, give statusopdateringer eller tilbyde offentlig anerkendelse.

Vi accepterer en indledende rapport sendt via almindelig e-mail eller en anden kanal. Hvis exploit-kode, legitimationsoplysninger, personoplysninger, kundekonfigurationer eller andre følsomme oplysninger skal udveksles, vil SALUS Controls PLC tilbyde en tilgængelig sikker metode til den videre kommunikation. At den rapporterende part ikke kan eller vælger ikke at anvende kryptering, medfører ikke i sig selv, at rapporten afvises.

4. Oplysninger, der skal medtages

For at hjælpe os med at undersøge din rapport effektivt bedes du, hvor det er muligt, medtage:

- Produktnavn og model
- Firmware- eller softwareversion
- Beskrivelse af sårbarheden
- Trin til at reproducere problemet
- Forventet og faktisk adfærd
- Potentiel sikkerhedsmæssig påvirkning
- Skærmbilleder, logfiler eller proof-of-concept, hvis tilgængeligt
- Dine foretrukne kontaktoplysninger til opfølgning

Undgå venligst at medtage følsomme personoplysninger, medmindre det er nødvendigt for at påvise sårbarheden.

Angiv også, hvor det er kendt, om problemet er offentligt kendt, aktivt udnyttes, har påvirket brugere eller er blevet rapporteret til en anden leverandør, producent eller koordinator. Du behøver ikke at oplyse alle de efterspurgte oplysninger, for at vi kan acceptere og registrere en rapport.

Under koordineret offentliggørelse begrænses adgangen til ikke-offentlige oplysninger om sårbarheder efter need-to-know-princippet. SALUS Controls PLC kan dele nødvendige oplysninger med produktteams, leverandører, koordinatorer, berørte parter eller kompetente myndigheder med henblik på validering, afhjælpning, brugerbeskyttelse og overholdelse af retlige forpligtelser under passende fortroligheds- og databeskyttelsesforanstaltninger.

Personoplysninger, der indsendes sammen med en sårbarhedsrapport, behandles i overensstemmelse med SALUS Controls PLCs gældende privatlivspolitik. Se venligst URL-adressen til privatlivspolitikken: https://saluscontrols.com/dk/privatlivspolitik-cookies/.

5. Responsproces

Efter modtagelse af din rapport vil SALUS Controls PLC:

- Bekræfte modtagelsen inden for tre arbejdsdage og under alle omstændigheder senest inden for syv kalenderdage; hvor det er muligt, angive et unikt sags-ID og foreløbige statusoplysninger.
- Foretage en indledende vurdering inden for syv arbejdsdage
- Validere den rapporterede sårbarhed
- Vurdere dens alvorlighed og potentielle påvirkning
- Udarbejde en plan for afhjælpning eller en sikkerhedsopdatering, hvor det er relevant
- Holde dig orienteret under hele undersøgelses- og afhjælpningsprocessen
- Mens en sag er aktiv, give en substantiel statusopdatering mindst én gang hver 30. kalenderdag og kommunikere hurtigere, når det bekræftede omfang, risikoen, afhjælpningsmetoden eller offentliggørelsesdatoen ændrer sig væsentligt.
- Hvis der kræves yderligere oplysninger, kan vi kontakte dig under vores undersøgelse.

6. Risikobaseret afhjælpning

Bekræftede sårbarheder prioriteres efter teknisk alvorlighed, udnyttelighed, berørte produkter, potentiel påvirkning, brugereksponering, dokumentation for aktiv udnyttelse, tilgængelige risikoreducerende tiltag og behov for sikker implementering. En numerisk score kan indgå i vurderingen, men afgør ikke alene prioriteten for afhjælpning.

SALUS Controls PLC fastsætter et sagsspecifikt mål for afhjælpning og kommunikerer væsentlige ændringer til den rapporterende part. Hvis øjeblikkelig afhjælpning ikke er mulig, kan passende risikoreducerende vejledning gives, før en permanent løsning er tilgængelig.

7. Koordineret offentliggørelse af sårbarheder

SALUS Controls PLC samarbejder med den rapporterende part og, hvor det er nødvendigt, leverandører, koordinatorer og andre berørte parter om at fastsætte en sagsspecifik offentliggørelsesdato. Tidspunktet kan ændres afhængigt af alvorlighed, aktiv udnyttelse, brugerrisiko, fremskridt med afhjælpning og implementering, afhængigheder i forsyningskæden samt gældende juridiske eller regulatoriske forpligtelser. Væsentlige ændringer af måldatoen meddeles relevante parter.

SALUS Controls PLC kan fremskynde brugerunderretning eller offentliggørelse, hvis en sårbarhed allerede er offentlig kendt, aktivt udnyttes, udgør en akut risiko for brugere, sandsynligvis vil blive lækket, eller hvis underretning kræves ved lov. Hvis en fuldstændig rettelse endnu ikke er tilgængelig, kan SALUS give midlertidig vejledning om risikoreduktion uden unødigt at muliggøre udnyttelse.

Oplysninger om afhjulpne sårbarheder offentliggøres i tilgængelige og menneskeligt læsbare sikkerhedsmeddelelser. Meddelelserne identificerer sårbarheden og de berørte produkter, offentliggørelses- og revisionsdatoer, potentiel påvirkning og alvorlighed, tilgængelig afhjælpning eller risikoreduktion, nødvendige brugerhandlinger og kontaktoplysninger. Meddelelser om tredjepartskomponenter kan henvise til autoritative upstream-oplysninger, når dette gør det muligt for brugere at afgøre, om SALUS-produkter er berørt.

Oplysninger om sårbarheder vil også blive gjort tilgængelige i et bredt anerkendt maskinlæsbart format, medmindre en begrundelse for ikke at gøre dette dokumenteres og godkendes. Offentliggørelse kan kun forsinkes eller udelades, hvis de relevante betingelser er blevet vurderet, dokumenteret og godkendt.

Hvor det kræves i henhold til gældende lovgivning eller er nødvendigt for at beskytte brugerne, vil SALUS Controls PLC informere berørte brugere og give tilgængelig vejledning om risikoreduktion eller korrigerende tiltag via passende tilgængelige kanaler.

8. Support til sikkerhedsopdateringer

SALUS Controls PLC leverer sikkerhedsopdateringer i hele den supportperiode, der er fastsat for hvert relevant produkt. Supportperioden fastsættes i overensstemmelse med gældende lovkrav under hensyntagen til produktets forventede brugsperiode, dets karakter og rimelige brugerforventninger.

Supportperioden vil være mindst fem år, medmindre produktet med rimelighed forventes at være i brug i en kortere periode, og den kan være længere, hvis dette er begrundet i produktets forventede levetid. Slutdatoen for den gældende supportperiode meddeles via de relevante produktoplysninger.

9. Uden for omfang

Alle potentielle sikkerhedsrapporter registreres og modtager en indledende vurdering. Forhold, der udelukkende er funktionelle, kommercielle eller supportrelaterede, kan henvises til den relevante supportkanal. Hvis et problem i første omgang ikke kan reproduceres, kan SALUS Controls PLC anmode om yderligere oplysninger og revurdere rapporten, når nye beviser bliver tilgængelige.

Teoretiske problemstillinger, scenarier med fysisk adgang, denial-of-service-forhold, social engineering-scenarier og afhængigheder af tredjeparter vurderes ud fra deres realistiske sikkerhedsmæssige påvirkning, udnyttelighed og produktets tilsigtede og med rimelighed forudsigelige anvendelse.

Sårbarheder i tredjepartskomponenter, der er integreret i, leveres med eller anvendes af et SALUS-produkt, er fortsat omfattet af SALUS' vurdering af produktpåvirkningen.

10. Ansvarlig sikkerhedsforskning

SALUS Controls PLC støtter ansvarlig sikkerhedsforskning udført i god tro. Vi beder forskere om at:

- Handle ansvarligt og etisk
- Undgå at forstyrre produkter, tjenester eller kunders drift
- Undgå at få adgang til, ændre eller slette kundedata
- Rapportere sårbarheder fortroligt gennem den proces, der er beskrevet i denne politik
- Give SALUS Controls PLC rimelig tid til at undersøge og afhjælpe problemet før offentliggørelse
- Overholde alle gældende love og regler under udførelse af sikkerhedsforskning

Når en rapporterende part handler i god tro, følger denne politik, undgår skade og rapporterer hurtigt, har SALUS Controls PLC ikke til hensigt at indlede retlige skridt alene på grund af sikkerhedsforskning udført efter denne politik. Erklæringen giver ikke adgang til tredjepartssystemer eller -data, binder ikke tredjepart eller myndigheder og fritager ikke den rapporterende part for at overholde gældende lov og indhente nødvendig tilladelse.

11. Kontakt

Ved sikkerhedsrelaterede rapporter eller spørgsmål om denne politik bedes du kontakte:

SALUS Controls PLC Sikkerhedsteam

E-mail: **security@saluscontrols.com**

12. Opdateringer af politikken

Denne politik gennemgås mindst årligt og efter væsentlige ændringer i lovkrav, rapporteringskanaler, produktomfang eller processer for sårbarhedshåndtering. Den aktuelle version, offentliggørelsesdato, seneste opdateringsdato og dokumentansvarlige fremgår af den offentliggjorte politik.

13. Anerkendelse

Med den rapporterende parts samtykke kan SALUS Controls PLC anerkende navn, alias eller organisation på en part, der indsender en gyldig sårbarhedsrapport og støtter koordineret offentliggørelse. Rapporter kan indsendes anonymt; fravalg af anerkendelse påvirker ikke accept, prioritering eller afhjælpningsbeslutninger.

Denne politik opretter ikke et bug bounty-program og garanterer ikke økonomiske eller andre belønninger.