Beleid inzake bekendmaking van kwetsbaarheden

Verantwoorde melding, onderzoek en verhelping van beveiligingskwetsbaarheden

Versie	Ingangsdatum	Documenteigenaar	Contact
1.0	September 2026	SALUS Controls PLC Security Team	security@saluscontrols.com

1. Inleiding

SALUS Controls PLC zet zich in voor de beveiliging van zijn producten, diensten en klanten. Wij verwelkomen verantwoorde meldingen van klanten, beveiligingsonderzoekers, partners, ontwikkelaars en andere leden van de beveiligingsgemeenschap die mogelijke beveiligingskwetsbaarheden identificeren die van invloed zijn op producten of diensten van SALUS Controls PLC.

Ons doel is om meldingen van mogelijke kwetsbaarheden tijdig te onderzoeken, gedurende het proces passend met de melder te communiceren en evenredige herstel- of beperkende maatregelen te treffen om gebruikers te beschermen.

Meld mogelijke beveiligingskwetsbaarheden vertrouwelijk via security@saluscontrols.com. SALUS Controls PLC bevestigt de ontvangst binnen drie werkdagen en in alle gevallen uiterlijk binnen zeven kalenderdagen. Deze ontvangstbevestiging bevestigt alleen dat de informatie is ontvangen en betekent niet dat het gemelde probleem als kwetsbaarheid is bevestigd.

2. Toepassingsgebied

Dit beleid is van toepassing op beveiligingskwetsbaarheden die betrekking hebben op:

- Producten van SALUS Controls PLC
- Firmware en software
- Mobiele applicaties
- Clouddiensten
- Openbaar toegankelijke webapplicaties en websites

Voor vragen over productinstallatie, configuratie, garantie of andere niet-beveiligingsgerelateerde onderwerpen kunt u contact opnemen met ons Customer Support-team via de gebruikelijke ondersteuningskanalen.

Wij accepteren beveiligingsmeldingen over SALUS-producten ongeacht hun levenscyclusstatus. Voor producten binnen de gepubliceerde periode voor beveiligingsondersteuning worden kwetsbaarheden en beveiligingsupdates behandeld in overeenstemming met de toepasselijke wettelijke verplichtingen. Voor producten buiten die periode zal SALUS Controls PLC meldingen nog steeds beoordelen en kan het, afhankelijk van het risico, de technische haalbaarheid en toepasselijke verplichtingen, beperkende maatregelen, migratieadvies of andere richtlijnen verstrekken.

3. Een kwetsbaarheid melden

Als u denkt dat u een beveiligingskwetsbaarheid hebt vastgesteld, meld deze dan vertrouwelijk per e-mail via security@saluscontrols.com. **security@saluscontrols.com**

Meldingen kunnen anoniem worden ingediend. Het ontbreken van een naam of een tweezijdige contactmethode verhindert de ontvangst of eerste beoordeling niet, maar kan onze mogelijkheid

beperken om aanvullende informatie op te vragen, statusupdates te verstrekken of openbare erkenning te bieden.

Wij accepteren een eerste melding die via gewone e-mail of een ander kanaal wordt verzonden. Als exploitcode, inloggegevens, persoonsgegevens, klantconfiguraties of andere gevoelige informatie moeten worden uitgewisseld, zal SALUS Controls PLC een beschikbare veilige methode aanbieden voor verdere communicatie. Het feit dat een melder geen versleuteling kan of wil gebruiken, is op zichzelf geen reden om de melding af te wijzen.

4. Op te nemen informatie

Om ons te helpen uw melding efficiënt te onderzoeken, verzoeken wij u waar mogelijk het volgende op te nemen:

- Productnaam en model
- Firmware- of softwareversie
- Beschrijving van de kwetsbaarheid
- Stappen om het probleem te reproduceren
- Verwacht en feitelijk gedrag
- Mogelijke beveiligingsimpact
- Screenshots, logbestanden of proof-of-concept, indien beschikbaar
- Uw voorkeurscontactgegevens voor opvolging

Vermijd het opnemen van gevoelige persoonsgegevens, tenzij dit noodzakelijk is om de kwetsbaarheid aan te tonen.

Geef waar bekend ook aan of het probleem openbaar is, actief wordt misbruikt, gebruikers heeft getroffen of bij een andere leverancier, aanbieder of coördinator is gemeld. U hoeft niet alle gevraagde informatie te verstrekken om een melding door ons te laten accepteren en registreren.

Tijdens gecoördineerde bekendmaking wordt de toegang tot niet-openbare informatie over kwetsbaarheden beperkt tot personen die deze informatie nodig hebben. SALUS Controls PLC kan noodzakelijke informatie delen met productteams, leveranciers, coördinatoren, getroffen partijen of bevoegde autoriteiten voor validatie, herstel, bescherming van gebruikers en naleving van wettelijke verplichtingen, met inachtneming van passende vertrouwelijkheids- en gegevensbeschermingsmaatregelen.

Persoonsgegevens die samen met een kwetsbaarheidsmelding worden ingediend, worden verwerkt in overeenstemming met de toepasselijke privacyverklaring van SALUS Controls PLC. Raadpleeg de URL van de privacyverklaring: https://saluscontrols.com/nl/privacy-cookies/.

5. Reactieproces

Na ontvangst van uw melding zal SALUS Controls PLC:

- De ontvangst binnen drie werkdagen en in alle gevallen uiterlijk binnen zeven kalenderdagen bevestigen; waar mogelijk met een uniek zaaknummer en voorlopige statusinformatie.
- Binnen zeven werkdagen een eerste beoordeling uitvoeren
- De gemelde kwetsbaarheid valideren
- De ernst en mogelijke impact beoordelen
- Waar passend een herstelplan of beveiligingsupdate ontwikkelen

- U gedurende het onderzoek- en herstelproces op de hoogte houden
- Zolang een zaak actief blijft, ten minste eenmaal per 30 kalenderdagen een inhoudelijke statusupdate verstrekken en eerder communiceren wanneer de bevestigde reikwijdte, het risico, de herstelaanpak of de datum van bekendmaking wezenlijk verandert.
- Als aanvullende informatie nodig is, kunnen wij tijdens ons onderzoek contact met u opnemen.

6. Risicogebaseerd herstel

Bevestigde kwetsbaarheden worden geprioriteerd op basis van technische ernst, misbruikbaarheid, getroffen producten, mogelijke impact, blootstelling van gebruikers, aanwijzingen voor actief misbruik, beschikbare beperkende maatregelen en de vereisten voor veilige implementatie. Een numerieke score kan de beoordeling ondersteunen, maar bepaalt op zichzelf niet de herstelprioriteit.

SALUS Controls PLC stelt per zaak een specifieke hersteldoelstelling vast en communiceert wezenlijke wijzigingen aan de melder. Wanneer onmiddellijk herstel niet mogelijk is, kunnen passende beperkende maatregelen of richtlijnen voor risicovermindering worden verstrekt voordat een permanente oplossing beschikbaar is.

7. Gecoördineerde bekendmaking van kwetsbaarheden

SALUS Controls PLC werkt samen met de melder en, waar nodig, leveranciers, coördinatoren en andere getroffen partijen om per zaak een specifieke datum voor bekendmaking vast te stellen. De timing kan worden herzien op basis van de ernst, actief misbruik, risico voor gebruikers, voortgang van herstel en implementatie, afhankelijkheden in de toeleveringsketen en toepasselijke wettelijke of regelgevende verplichtingen. Wezenlijke wijzigingen in de streefdatum worden aan de relevante partijen gecommuniceerd.

SALUS Controls PLC kan de kennisgeving aan gebruikers of openbare bekendmaking versnellen wanneer een kwetsbaarheid al openbaar is, actief wordt misbruikt, een dringend risico voor gebruikers vormt, waarschijnlijk zal uitlekken of wanneer kennisgeving wettelijk verplicht is. Wanneer nog geen volledige oplossing beschikbaar is, kan SALUS tijdelijke beperkende maatregelen of richtlijnen voor risicovermindering verstrekken zonder misbruik onnodig mogelijk te maken.

Informatie over verholpen kwetsbaarheden wordt gepubliceerd in toegankelijke, voor mensen leesbare beveiligingsadviezen. Deze adviezen vermelden de kwetsbaarheid en getroffen producten, publicatie- en revisiedata, mogelijke impact en ernst, beschikbare herstel- of beperkende maatregelen, vereiste acties van gebruikers en contactinformatie. Adviezen over componenten van derden kunnen verwijzen naar gezaghebbende broninformatie wanneer dit gebruikers in staat stelt te bepalen of SALUS-producten zijn getroffen.

Informatie over kwetsbaarheden wordt ook beschikbaar gesteld in een algemeen erkend machineleesbaar formaat, tenzij een motivering om dit niet te doen is gedocumenteerd en goedgekeurd. Publicatie mag alleen worden uitgesteld of achterwege gelaten wanneer de toepasselijke voorwaarden zijn beoordeeld, gedocumenteerd en goedgekeurd.

Waar dit volgens de toepasselijke wetgeving vereist of noodzakelijk is om gebruikers te beschermen, zal SALUS Controls PLC getroffen gebruikers informeren en beschikbare beperkende of corrigerende richtlijnen verstrekken via passende toegankelijke kanalen.

8. Ondersteuning voor beveiligingsupdates

SALUS Controls PLC levert beveiligingsupdates gedurende de ondersteuningsperiode die voor elk toepasselijk product is vastgesteld. De ondersteuningsperiode wordt bepaald in overeenstemming met de toepasselijke wettelijke vereisten, rekening houdend met de verwachte gebruiksduur van het product, de aard ervan en redelijke verwachtingen van gebruikers.

De ondersteuningsperiode bedraagt ten minste vijf jaar, tenzij redelijkerwijs wordt verwacht dat het product gedurende een kortere periode wordt gebruikt, en kan langer zijn wanneer dit wordt gerechtvaardigd door de verwachte levensduur van het product. De toepasselijke einddatum van de ondersteuningsperiode wordt via de relevante productinformatie gecommuniceerd.

9. Buiten toepassingsgebied

Alle mogelijke beveiligingsmeldingen worden geregistreerd en krijgen een eerste beoordeling. Problemen die uitsluitend functioneel, commercieel of ondersteuningsgerelateerd zijn, kunnen naar het juiste ondersteuningskanaal worden doorverwezen. Als een probleem aanvankelijk niet kan worden gereproduceerd, kan SALUS Controls PLC aanvullende informatie opvragen en de melding opnieuw beoordelen wanneer nieuw bewijs beschikbaar komt.

Theoretische problemen, scenario's met fysieke toegang, denial-of-service-omstandigheden, social-engineering-scenario's en afhankelijkheden van derden worden beoordeeld op basis van hun realistische beveiligingsimpact, misbruikbaarheid en het beoogde en redelijkerwijs voorzienbare gebruik van het product.

Kwetsbaarheden in componenten van derden die in een SALUS-product zijn geïntegreerd, ermee worden geleverd of waarop het product steunt, blijven onderworpen aan de productimpactbeoordeling van SALUS.

10. Verantwoord beveiligingsonderzoek

SALUS Controls PLC ondersteunt verantwoord beveiligingsonderzoek dat te goeder trouw wordt uitgevoerd. Wij verzoeken onderzoekers om:

- Verantwoord en ethisch te handelen
- Verstoring van producten, diensten of klantactiviteiten te vermijden
- Toegang tot, wijziging of verwijdering van klantgegevens te vermijden
- Kwetsbaarheden vertrouwelijk te melden via het in dit beleid beschreven proces
- SALUS Controls PLC een redelijke termijn te geven om het probleem te onderzoeken en te verhelpen vóór openbare bekendmaking
- Alle toepasselijke wet- en regelgeving na te leven tijdens beveiligingsonderzoek

Wanneer een melder te goeder trouw handelt, dit beleid naleeft, schade vermijdt en tijdig meldt, is SALUS Controls PLC niet voornemens juridische stappen te ondernemen uitsluitend vanwege beveiligingsonderzoek dat overeenkomstig dit beleid is uitgevoerd. Deze verklaring geeft geen toestemming voor toegang tot systemen of gegevens van derden, bindt geen derde partij of autoriteit en ontslaat de melder niet van de verplichting om toepasselijke wetgeving na te leven en vereiste toestemming te verkrijgen.

11. Contact

Voor alle beveiligingsgerelateerde meldingen of vragen over dit beleid kunt u contact opnemen met:

SALUS Controls PLC Security Team

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

12. Beleidsupdates

Dit beleid wordt ten minste jaarlijks herzien en na wezenlijke wijzigingen in toepasselijke wettelijke vereisten, meldingskanalen, productomvang of processen voor de behandeling van kwetsbaarheden. De huidige versie, publicatiedatum, datum van laatste wijziging en beleidseigenaar worden bij het gepubliceerde beleid weergegeven.

13. Erkenning

Met toestemming van de melder kan SALUS Controls PLC de naam, alias of organisatie erkennen van een melder die een geldige kwetsbaarheidsmelding indient en gecoördineerde bekendmaking ondersteunt. Meldingen kunnen anoniem worden ingediend en het afzien van erkenning heeft geen invloed op acceptatie, prioritering of herstelbeslissingen.

Dit beleid stelt geen bug bounty in en garandeert geen financiële of andere beloningen.