Policy för rapportering av sårbarheter

Ansvarsfull rapportering, utredning och åtgärd av säkerhetssårbarheter

Version	Giltighetsdatum	Dokumentägare	Kontakt
1.0	September 2026	SALUS Controls PLC:s säkerhetsteam	security@saluscontrols.com

1. Inledning

SALUS Controls PLC arbetar för att skydda säkerheten i sina produkter och tjänster samt för sina kunder. Vi välkomnar ansvarsfulla rapporter från kunder, säkerhetsforskare, partners, utvecklare och andra inom säkerhetsområdet som identifierar potentiella säkerhetssårbarheter som påverkar SALUS Controls PLC:s produkter eller tjänster.

Vårt mål är att skyndsamt utreda rapporter om potentiella sårbarheter, kommunicera på lämpligt sätt med rapportören under hela processen och vidta proportionerliga åtgärder eller riskreducerande åtgärder för att skydda användarna.

Rapportera potentiella säkerhetssårbarheter konfidentiellt till security@saluscontrols.com. SALUS Controls PLC bekräftar mottagandet inom tre arbetsdagar och alltid senast inom sju kalenderdagar. Bekräftelsen innebär endast att informationen har mottagits och betyder inte att det rapporterade problemet har bekräftats som en sårbarhet.

2. Omfattning

Denna policy gäller säkerhetssårbarheter som påverkar:

- SALUS Controls PLC:s produkter
- Firmware och programvara
- Mobilapplikationer
- Molntjänster
- Allmänt tillgängliga webbapplikationer och webbplatser

För frågor om produktinstallation, konfiguration, garanti eller andra ärenden som inte gäller säkerhet, kontakta vår kundsupport via de ordinarie supportkanalerna.

Vi tar emot säkerhetsrapporter om SALUS-produkter oavsett var produkten befinner sig i sin livscykel. För produkter inom den publicerade säkerhetssupportperioden hanteras sårbarheter och säkerhetsuppdateringar i enlighet med tillämpliga rättsliga krav. För produkter utanför denna period kommer SALUS Controls PLC fortfarande att bedöma rapporter och kan lämna riskreducerande åtgärder, migreringsråd eller annan vägledning utifrån risk, teknisk genomförbarhet och tillämpliga skyldigheter.

3. Rapportera en sårbarhet

Om du tror att du har identifierat en säkerhetssårbarhet, rapportera den konfidentiellt via e-post till**security@saluscontrols.com**

Rapporter kan lämnas anonymt. Avsaknad av namn eller möjlighet till tvåvägskommunikation hindrar inte mottagande eller inledande bedömning, men kan begränsa vår möjlighet att begära ytterligare information, lämna statusuppdateringar eller ge offentligt erkännande.

Vi tar emot en första rapport via vanlig e-post eller annan kanal. Om exploitkod, inloggningsuppgifter, personuppgifter, kundkonfigurationer eller annan känslig information behöver utbytas erbjuder SALUS Controls PLC en tillgänglig säker metod för fortsatt kommunikation. Att rapportören inte kan eller väljer att inte använda kryptering leder i sig inte till att rapporten avvisas.

4. Information som bör ingå

För att hjälpa oss att utreda din rapport effektivt, inkludera om möjligt:

- Produktnamn och modell
- Firmware- eller programvaruversion
- Beskrivning av sårbarheten
- Steg för att återskapa problemet
- Förväntat och faktiskt beteende
- Möjlig säkerhetspåverkan
- Skärmbilder, loggar eller proof-of-concept, om tillgängligt
- Önskade kontaktuppgifter för uppföljning

Undvik att inkludera känsliga personuppgifter om de inte behövs för att visa sårbarheten.

Ange även, om du känner till det, om problemet är offentligt, utnyttjas aktivt, har påverkat användare eller har rapporterats till en annan leverantör, tillverkare eller samordnare. Du behöver inte lämna alla efterfrågade uppgifter för att vi ska kunna ta emot och registrera rapporten.

Vid samordnad offentliggörande begränsas åtkomsten till icke-offentlig information om sårbarheter enligt behovsprincipen. SALUS Controls PLC kan dela nödvändig information med produktteam, leverantörer, samordnare, berörda parter eller behöriga myndigheter för validering, åtgärd, användarskydd och efterlevnad av rättsliga skyldigheter, med lämpliga kontroller för sekretess och dataskydd.

Personuppgifter som lämnas tillsammans med en sårbarhetsrapport behandlas i enlighet med SALUS Controls PLC:s tillämpliga integritetsmeddelande. Se integritetspolicyn på: https://saluscontrols.com/se/webbplats-integritet-cookies/.

5. Hanteringsprocess

Efter att ha tagit emot din rapport kommer SALUS Controls PLC att:

- Bekräfta mottagandet inom tre arbetsdagar och alltid senast inom sju kalenderdagar samt, om möjligt, ange ett unikt ärendenummer och preliminär statusinformation.
- Genomföra en inledande bedömning inom sju arbetsdagar
- Validera den rapporterade sårbarheten
- Bedöma dess allvarlighetsgrad och möjliga påverkan
- Ta fram en åtgärdsplan eller säkerhetsuppdatering när det är lämpligt
- Hålla dig informerad under utrednings- och åtgärdsprocessen
- Så länge ärendet är aktivt lämna en innehållsmässig statusuppdatering minst var 30:e kalenderdag och kommunicera tidigare om bekräftad omfattning, risk, åtgärdsmetod eller datum för offentliggörande ändras väsentligt.
- Om ytterligare information behövs kan vi kontakta dig under utredningen.

6. Riskbaserad åtgärd

Bekräftade sårbarheter prioriteras utifrån teknisk allvarlighetsgrad, möjligheten att utnyttja dem, berörda produkter, möjlig påverkan, användarexponering, tecken på aktivt utnyttjande, tillgängliga riskreducerande åtgärder och behov av säker distribution. Ett numeriskt poängvärde kan stödja bedömningen men avgör inte ensamt prioriteringen.

SALUS Controls PLC fastställer ett ärendespecifikt mål för åtgärd och kommunicerar väsentliga ändringar till rapportören. När omedelbar åtgärd inte är möjlig kan lämpliga riskreducerande åtgärder eller vägledning lämnas innan en permanent korrigering finns tillgänglig.

7. Samordnat offentliggörande av sårbarheter

SALUS Controls PLC samarbetar med rapportören och vid behov med leverantörer, samordnare och andra berörda parter för att fastställa ett ärendespecifikt datum för offentliggörande. Tidpunkten kan ändras utifrån allvarlighetsgrad, aktivt utnyttjande, risk för användare, framsteg i åtgärd och distribution, beroenden i leveranskedjan samt tillämpliga rättsliga eller regulatoriska krav. Väsentliga ändringar av måldatumet kommuniceras till berörda parter.

SALUS Controls PLC kan påskynda användarinformation eller offentligt offentliggörande om en sårbarhet redan är offentlig, utnyttjas aktivt, innebär en akut risk för användare, sannolikt kommer att läcka eller om information krävs enligt lag. Om en fullständig korrigering ännu inte finns kan SALUS lämna tillfälliga riskreducerande åtgärder utan att i onödan underlätta utnyttjande.

Information om åtgärdade sårbarheter publiceras i tillgängliga och lättlästa säkerhetsmeddelanden. Meddelandena anger sårbarheten och berörda produkter, publicerings- och revisionsdatum, möjlig påverkan och allvarlighetsgrad, tillgängliga åtgärder eller riskreducerande åtgärder, nödvändiga användaråtgärder och kontaktinformation. Meddelanden om tredjepartskomponenter kan hänvisa till auktoritativ information från ursprungskällan när detta gör det möjligt för användare att avgöra om SALUS-produkter påverkas.

Information om sårbarheter görs även tillgänglig i ett allmänt vedertaget maskinläsbart format, om inte ett skäl för att avstå dokumenteras och godkänns. Publicering får endast skjutas upp eller utelämnas när tillämpliga villkor har bedömts, dokumenterats och godkänts.

När det krävs enligt tillämplig lag eller är nödvändigt för att skydda användare informerar SALUS Controls PLC berörda användare och tillhandahåller tillgängliga riskreducerande eller korrigerande råd via lämpliga och tillgängliga kanaler.

8. Support för säkerhetsuppdateringar

SALUS Controls PLC tillhandahåller säkerhetsuppdateringar under den supportperiod som fastställts för varje berörd produkt. Supportperioden bestäms i enlighet med tillämpliga rättsliga krav med hänsyn till produktens förväntade användningstid, dess egenskaper och användarnas rimliga förväntningar.

Supportperioden är minst fem år, om produkten inte rimligen förväntas användas under en kortare tid, och kan vara längre när detta motiveras av produktens förväntade livslängd. Slutdatum för den tillämpliga supportperioden meddelas i relevant produktinformation.

9. Utanför omfattningen

Alla potentiella säkerhetsrapporter registreras och får en inledande bedömning. Frågor som enbart gäller funktion, handel eller support kan hänvisas till lämplig supportkanal. Om ett problem inte kan återskapas inledningsvis kan SALUS Controls PLC begära ytterligare information och ompröva rapporten när nya bevis finns tillgängliga.

Teoretiska problem, scenarier med fysisk åtkomst, överbelastningsattacker, social manipulation och beroenden av tredje part bedöms utifrån realistisk säkerhetspåverkan, möjlighet till utnyttjande samt produktens avsedda och rimligen förutsebara användning.

Sårbarheter i tredjepartskomponenter som är integrerade i, levereras med eller används av en SALUS-produkt omfattas fortsatt av SALUS bedömning av produktpåverkan.

10. Ansvarsfull säkerhetsforskning

SALUS Controls PLC stödjer ansvarsfull säkerhetsforskning som bedrivs i god tro. Vi ber forskare att:

- Agera ansvarsfullt och etiskt
- Undvika att störa produkter, tjänster eller kundverksamhet
- Undvika att komma åt, ändra eller radera kunddata
- Rapportera sårbarheter konfidentiellt enligt processen i denna policy
- Ge SALUS Controls PLC rimlig tid att utreda och åtgärda problemet före offentligt offentliggörande
- Följa alla tillämpliga lagar och regler under säkerhetsforskningen

När en rapportör agerar i god tro, följer denna policy, undviker skada och rapporterar skyndsamt avser SALUS Controls PLC inte att inleda rättsliga åtgärder enbart på grund av säkerhetsforskning som genomförts i enlighet med denna policy. Uttalandet ger inte tillstånd till åtkomst till tredje parts system eller data, binder inte tredje part eller myndighet och befriar inte rapportören från skyldigheten att följa tillämplig lag och inhämta nödvändiga tillstånd.

11. Kontakt

För alla säkerhetsrelaterade rapporter eller frågor om denna policy, kontakta:

SALUS Controls PLC:s säkerhetsteam

E-post: security@saluscontrols.com

12. Uppdateringar av policyn

Denna policy granskas minst årligen och efter väsentliga ändringar av tillämpliga rättsliga krav, rapporteringskanaler, produktomfattning eller processer för sårbarhetshantering. Den aktuella versionen, publiceringsdatumet, datumet för senaste uppdatering och policyägaren visas tillsammans med den publicerade policyn.

13. Erkännande

Med rapportörens samtycke kan SALUS Controls PLC uppmärksamma namn, alias eller organisation för en rapportör som lämnar en giltig sårbarhetsrapport och stödjer samordnat offentliggörande. Rapporter kan lämnas anonymt, och att avstå från erkännande påverkar inte mottagande, prioritering eller åtgärd.

Policyn är inget bug bounty-program och garanterar inte ekonomisk eller annan ersättning.