

SALUS Controls PLC - Formulär för rapportering av misstänkt sårbarhet

Använd detta formulär för att rapportera en misstänkt säkerhetssårbarhet som påverkar en SALUS-produkt, applikation, molntjänst eller webbplats.

Fyll i så mycket information som möjligt. Du behöver inte fylla i alla fält för att vi ska kunna ta emot din rapport.

Du kan lämna in en rapport anonymt. Om du inte anger kontaktuppgifter kan vi dock sakna möjlighet att begära ytterligare information eller ge dig uppdateringar om rapporten.

När formuläret är ifyllt, skicka det till security@saluscontrols.com.

Ange inte lösenord, autentiseringstoken, privata nycklar eller onödiga person- eller kunduppgifter.

Fält märkta "Obligatoriskt" är endast obligatoriska när informationen rimligen finns tillgänglig. Du kan lämna in rapporten även om du inte har all information.

Rapport om misstänkt sårbarhet

1. Uppgifter om rapportören

Fält	Svar
Namn eller alias (valfritt)	
Organisation (valfritt)	
E-post/kontaktmetod (obligatoriskt om du inte rapporterar anonymt)	
Önskat språk (valfritt)	
Rapporterar du anonymt?	☐ Ja ☐ Nej

2. Berörd produkt eller komponent

Fält	Svar
Produkt- eller tjänstenamn (obligatoriskt)	
Modell (om tillämpligt)	
Maskinvaruversion (om känd)	
Version av firmware/programvara/applikation (om känd)	
Land/region	

Fält	Svar
Annan relevant konfigurationsinformation	

3. Beskrivning av den misstänkta sårbarheten

Fält	Svar
Kort rubrik (obligatoriskt)	
Beskriv säkerhetsproblemet som du har identifierat (obligatoriskt)	
När upptäckte du problemet första gången?	
Vad förväntade du dig skulle hända?	
Vad hände i stället?	
Kan du återskapa problemet?	☐ Ja ☐ Nej ☐ Ibland ☐ Okänt
Beskriv om möjligt stegen som krävs för att återskapa problemet:	
Vilken säkerhetspåverkan bedömer du att problemet kan ha?	
Bifogas bilagor? Du kan bifoga relevanta skärmbilder, loggar, videor eller proof-of-concept-information.	☐ Ja ☐ Nej

Ytterligare teknisk information (valfritt – för säkerhetsforskare)

Fält	Svar
Typ av sårbarhet (kringgående av autentisering, injektion, minneskorruption osv.), om känd	
CWE/CVE, om känt	
Teknisk orsak/detaljer	
Testmiljö/konfiguration	
Proof of concept	

4. Angreppsscenario

Angreppsscenariot skiljer sig från stegen för att återskapa problemet. Beskriv hur en realistisk angripare skulle kunna utnyttja sårbarheten.

Fält	Svar
Beskriv, om det är känt, hur någon skulle kunna utnyttja denna sårbarhet	
Angriparens åtkomst	☐ Remote network ☐ Adjacent network ☐ Local network ☐ Local device ☐ Physical access ☐ Okänt
Användarinteraktion krävs	☐ Ja ☐ Nej ☐ Okänt
Särskilda behörigheter/konto krävs	☐ Ja ☐ Nej ☐ Okänt Om ja, beskriv vilka behörigheter/vilket konto som krävs:

5. Konsekvensbedömning (valfritt)

Fyll i detta avsnitt om du kan bedöma den potentiella påverkan.

Påverkansområde	Rapportörens bedömning
Konfidentialitet	☐ Nejne ☐ Låg ☐ Medel ☐ Hög ☐ Okänt
Integritet	☐ Nejne ☐ Låg ☐ Medel ☐ Hög ☐ Okänt
Tillgänglighet	☐ Nejne ☐ Låg ☒ Medel ☐ Hög ☐ Okänt
Säkerhet	☐ Nejne ☐ Låg ☐ Medel ☐ Hög ☐ Okänt
Integritetsskydd	☐ Nejne ☐ Låg ☐ Medel ☐ Hög ☐ Okänt
Påverkan på leveranskedjan eller det bredare ekosystemet	☐ Ingen ☐ Låg ☐ Medel ☐ Hög ☐ Okänd
Föreslagen allvarlighetsgrad, om tillgänglig (valfritt)	☐ Låg ☐ Medel ☐ Hög ☐ Kritisk ☐ Okänd
CVSS-vektor, om tillgänglig (valfritt)	

6. Status för utnyttjande och offentliggörande

Fält	Svar
Är sårbarheten redan offentlig?	☐ Nej ☐ Ja ☐ Okänt Om ja, ange URL och datum:
Finns ett offentligt proof of concept?	☐ Nej ☐ Ja ☐ Okänt Om ja, ange URL och datum:
Är aktivt utnyttjande känt eller misstänkt?	☐ Nej ☐ Ja ☐ Okänt Om ja, ange detaljer:
Har någon annan leverantör, underleverantör, CERT eller samordnare kontaktats?	☐ Nej ☐ Ja ☐ Okänt If yes, please provide party, case ID and date:
Planerar du att diskutera eller publicera problemet efter att det har åtgärdats?	☐ Nej ☐ Ja ☐ Okänt Om ja, ange detaljer:
Önskat datum för samordnat offentliggörande, om tillämpligt	

Information om samordnat offentliggörande:

Håll icke-offentlig information om sårbarheten konfidentiell fram till det överenskomna datumet för offentliggörande. Om risken förändras, aktivt utnyttjande observeras eller offentliggörande blir sannolikt, kontakta omgående security@saluscontrols.com så att planen för offentliggörande kan omprövas. security@saluscontrols.com

7. Föreslagen åtgärd eller riskreducering (valfritt)

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

8. Önskemål om erkännande

Val	Svar
Får vi offentligt uppmärksamma dig om en säkerhetsrekommendation publiceras?	☐ Ja ☐ Nej
Visningsnamn, alias eller organisation	
Önskad profil- eller referenslänk, om detta tillåts enligt policyn	

9. Bilagor och ytterligare information

Lista alla filer som bifogas rapporten. Ange inte lösenord, autentiseringstoken, privata nycklar eller onödiga person- eller kunduppgifter.

Fält	Svar
Är filer bifogade till rapporten?	☐ Ja ☐ Nej
Type of files attached	☐ Screenshots ☐ Logs ☐ Video ☐ Proof of concept ☐ Packet capture ☐ Other
Beskrivning av bifogade filer	
Ytterligare information som är relevant för rapporten	
Krav på konfidentialitet eller hantering	

Om du bifogar loggar, skärmbilder, videor, paketfångster eller proof-of-concept-material ska du ta bort onödiga personuppgifter, kunduppgifter, lösenord, autentiseringstoken, privata nycklar eller annan känslig information innan rapporten skickas in.

10. Bekräftelse om god tro

Genom att skicka in rapporten bekräftar rapportören, såvitt denne känner till, att:

- ☐ Rapporten är korrekt och har tagits fram genom säkerhetsforskning i god tro.
- ☐ Testningen begränsades till system, enheter, konton och data som rapportören äger eller hade behörighet att testa.
- ☐ Onödig åtkomst till, lagring av eller spridning av icke-offentliga uppgifter undveks.
- ☐ Rapportören kommer att samordna offentliggörandet i enlighet med den publicerade policyn, med förbehåll för tillämplig lag och eventuella brådskande förändringar av risken för användare.
- ☐ Jag bekräftar att jag inte avsiktligt har inkluderat lösenord, autentiseringstoken, privata nycklar eller onödiga person- eller kunduppgifter.

Datum för inlämning: _____

Rapportörens namn eller alias, om angivet:

Så skickar du in rapporten

Skicka det ifyllda formuläret via e-post till: security@saluscontrols.com

Du kan även rapportera en misstänkt sårbarhet direkt via e-post utan att använda detta formulär. Vi rekommenderar att formuläret används eftersom det hjälper SALUS Controls PLC att samla in den information som behövs för att bedöma rapporten effektivt.