

SALUS Controls PLC - Formular zur Meldung einer vermuteten Sicherheitslücke

Verwenden Sie dieses Formular, um eine vermutete Sicherheitslücke zu melden, die ein SALUS Produkt, eine Anwendung, einen Cloud-Dienst oder eine Website betrifft.

Bitte machen Sie so viele Angaben wie möglich. Sie müssen nicht jedes Feld ausfüllen, damit wir Ihre Meldung entgegennehmen können.

Sie können eine Meldung anonym einreichen. Wenn Sie jedoch keine Kontaktdaten angeben, können wir möglicherweise keine zusätzlichen Informationen anfordern oder Sie über den Stand Ihrer Meldung informieren.

Bitte senden Sie das ausgefüllte Formular an security@saluscontrols.com.

Bitte geben Sie keine Passwörter, Authentifizierungstoken, privaten Schlüssel oder unnötigen personenbezogenen Daten bzw. Kundendaten an.

Mit „Erforderlich“ gekennzeichnete Felder sind nur auszufüllen, soweit die Informationen vernünftigerweise verfügbar sind. Auch wenn Ihnen nicht alle Informationen vorliegen, können Sie die Meldung einreichen.

Meldung einer vermuteten Sicherheitslücke

1. Angaben zur meldenden Person

Feld	Antwort
Name oder Alias (optional)	
Organisation (optional)	
E-Mail/Kontaktmöglichkeit (erforderlich, sofern nicht anonym gemeldet wird)	
Bevorzugte Sprache (optional)	
Anonyme Meldung?	☐ Ja ☐ Nein

2. Betroffenes Produkt oder betroffene Komponente

Feld	Antwort
Produkt- oder Dienstname (erforderlich)	
Modell (falls zutreffend)	
Hardwareversion (sofern bekannt)	

Feld	Antwort
Firmware-/Software-/Anwendungsversion (sofern bekannt)	
Land/Region	
Weitere relevante Konfigurationsinformationen	

3. Beschreibung der vermuteten Sicherheitslücke

Feld	Antwort
Kurztitel (erforderlich)	
Bitte beschreiben Sie das festgestellte Sicherheitsproblem (erforderlich)	
Wann haben Sie das Problem erstmals festgestellt?	
Was hätten Sie erwartet?	
Was ist tatsächlich passiert?	
Können Sie das Problem reproduzieren?	☐ Ja ☐ Nein ☐ Manchmal ☐ Unbekannt
Beschreiben Sie nach Möglichkeit die zur Reproduktion erforderlichen Schritte:	
Welche Auswirkungen auf die Sicherheit könnte das Problem Ihrer Einschätzung nach haben?	
Anhänge beigefügt? Sie können relevante Screenshots, Protokolle, Videos oder Proof-of-Concept-Informationen beifügen.	☐ Ja ☐ Nein

Zusätzliche technische Informationen (optional – für Sicherheitsforschende)

Feld	Antwort
Art der Sicherheitslücke (Umgehung der Authentifizierung, Injection, Speicherfehler usw.), sofern bekannt	
CWE/CVE, sofern bekannt	
Technische Ursache / Details	
Testumgebung / Konfiguration	

Feld	Antwort
Proof of Concept	

4. Angriffsszenario

Das Angriffsszenario unterscheidet sich von den Schritten zur Reproduktion. Beschreiben Sie, wie ein realistischer Angreifer die Sicherheitslücke ausnutzen könnte.

Feld	Antwort
Sofern bekannt, beschreiben Sie bitte, wie diese Sicherheitslücke ausgenutzt werden könnte	
Zugriff des Angreifers	☐ Entferntes Netzwerk ☐ Benachbartes Netzwerk ☐ Local network ☐ Local device ☐ Physical access ☐ Unbekannt
Benutzerinteraktion erforderlich	☐ Ja ☐ Nein ☐ Unbekannt
Besondere Berechtigungen/Konto erforderlich	☐ Ja ☐ Nein ☐ Unbekannt Falls ja, beschreiben Sie bitte die erforderlichen Berechtigungen/das erforderliche Konto:

5. Bewertung der Auswirkungen (optional)

Füllen Sie diesen Abschnitt aus, wenn Sie die möglichen Auswirkungen einschätzen können.

Auswirkungsbereich	Einschätzung der meldenden Person
Vertraulichkeit	☐ Neinne ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt
Integrität	☐ Neinne ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt
Verfügbarkeit	☐ Neinne ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt
Sicherheit	☐ Neinne ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt
Datenschutz	☐ Neinne ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt
Auswirkungen auf die Lieferkette oder das weitere Ökosystem	☐ Keine ☐ Niedrig ☐ Mittel ☐ Hoch ☐ Unbekannt

Auswirkungsbereich	Einschätzung der meldenden Person
Vorgeschlagener Schweregrad, sofern verfügbar (optional)	☐ Niedrig ☐ Mittel ☐ Hoch ☐ Kritisch ☐ Unbekannt
CVSS-Vektor, sofern verfügbar (optional)	

6. Status der Ausnutzung und Offenlegung

Feld	Antwort
Ist die Sicherheitslücke bereits öffentlich bekannt?	☐ Nein ☐ Ja ☐ Unbekannt Falls ja, geben Sie bitte URL und Datum an:
Ist ein Proof of Concept öffentlich verfügbar?	☐ Nein ☐ Ja ☐ Unbekannt Falls ja, geben Sie bitte URL und Datum an:
Ist eine aktive Ausnutzung bekannt oder wird sie vermutet?	☐ Nein ☐ Ja ☐ Unbekannt Falls ja, machen Sie bitte nähere Angaben:
Wurde ein anderer Hersteller, Lieferant, ein CERT oder eine koordinierende Stelle kontaktiert?	☐ Nein ☐ Ja ☐ Unbekannt Falls ja, geben Sie bitte Stelle, Fall-ID und Datum an:
Planen Sie, das Problem nach der Behebung zu besprechen oder zu veröffentlichen?	☐ Nein ☐ Ja ☐ Unbekannt Falls ja, machen Sie bitte nähere Angaben:
Bevorzugtes Datum für die koordinierte Offenlegung, falls vorhanden	

Hinweis zur koordinierten Offenlegung:

Bitte behandeln Sie nicht öffentliche Informationen zur Sicherheitslücke bis zu einem vereinbarten Offenlegungsdatum vertraulich. Wenn sich das Risiko ändert, eine aktive Ausnutzung beobachtet wird oder eine öffentliche Offenlegung wahrscheinlich wird, kontaktieren Sie bitte umgehend security@saluscontrols.com, damit der Offenlegungsplan neu bewertet werden kann.

7. Vorgeschlagene Behebung oder Risikominderung (optional)

- Vorgeschlagene Behebung der Ursache, sofern bekannt: _____
- Vorgeschlagene vorübergehende Risikominderung oder Umgehungslösung, sofern bekannt: ____
- Relevante Branchenpraxis, Schutzregel oder Referenz: _____

8. Präferenz zur öffentlichen Nennung

Auswahl	Antwort
Dürfen wir Sie öffentlich nennen, wenn eine Sicherheitsmitteilung veröffentlicht wird?	☐ Ja ☐ Nein

Auswahl	Antwort
Anzuzeigender Name, Alias oder Organisation	
Bevorzugter Profil- oder Referenzlink, sofern gemäß Richtlinie zulässig	

9. Anhänge und zusätzliche Informationen

Bitte listen Sie alle Dateien auf, die Ihrer Meldung beigelegt sind. Geben Sie keine Passwörter, Authentifizierungstoken, privaten Schlüssel oder unnötigen personenbezogenen Daten bzw. Kundendaten an.

Feld	Antwort
Sind dieser Meldung Dateien beigelegt?	☐ Ja ☐ Nein
Art der beigelegten Dateien	☐ Screenshots ☐ Protokolle ☐ Video ☐ Proof of Concept ☐ Paketmitschnitt ☐ Sonstiges
Beschreibung der beigelegten Dateien	
Weitere für die Meldung relevante Informationen	
Anforderungen an Vertraulichkeit oder Handhabung	

Wenn Sie Protokolle, Screenshots, Videos, Paketmitschnitte oder Proof-of-Concept-Material beifügen, entfernen Sie bitte vor dem Einreichen der Meldung unnötige personenbezogene Daten, Kundendaten, Passwörter, Authentifizierungstoken, private Schlüssel oder andere sensible Informationen.

10. Bestätigung nach Treu und Glauben

Mit dem Einreichen dieser Meldung bestätigt die meldende Person nach bestem Wissen, dass:

- ☐ Die Meldung zutreffend ist und im Rahmen von Sicherheitsforschung nach Treu und Glauben erstellt wurde.
- ☐ die Tests auf Systeme, Geräte, Konten und Daten beschränkt waren, die der meldenden Person gehören oder zu deren Test sie berechtigt war.
- ☐ unnötiger Zugriff auf, Speicherung von oder Offenlegung nicht öffentlicher Daten vermieden wurde.
- ☐ die meldende Person die Offenlegung gemäß der veröffentlichten Richtlinie koordiniert, vorbehaltlich des anwendbaren Rechts und dringender Änderungen des Risikos für Nutzer.
- ☐ Ich bestätige, dass ich nicht absichtlich Passwörter, Authentifizierungstoken, private Schlüssel oder unnötige personenbezogene Daten bzw. Kundendaten angegeben habe.

Einreichungsdatum: _____

Name oder Alias der meldenden Person, sofern angegeben:

So reichen Sie diese Meldung ein

Bitte senden Sie das ausgefüllte Formular per E-Mail an: security@saluscontrols.com

Sie können eine vermutete Sicherheitslücke auch direkt per E-Mail melden, ohne dieses Formular zu verwenden. Die Verwendung dieses Formulars wird empfohlen, da SALUS Controls PLC damit die für eine effiziente Bewertung der Meldung erforderlichen Informationen erfassen kann.