Richtlinie zur Offenlegung von Schwachstellen

Verantwortungsvolle Meldung, Prüfung und Behebung von Sicherheitslücken

Version	Gültig ab	Dokumentverantwortlicher	Kontakt
1.0	September 2026	SALUS Controls PLC Security Team	security@saluscontrols.com

1. Einleitung

SALUS Controls PLC schützt die Sicherheit seiner Produkte, Dienstleistungen und Kunden. Wir begrüßen verantwortungsvolle Meldungen von Kunden, Sicherheitsforschern, Partnern, Entwicklern und anderen Mitgliedern der Sicherheitsgemeinschaft zu möglichen Sicherheitslücken in Produkten oder Dienstleistungen von SALUS Controls PLC.

Unser Ziel ist es, mögliche Schwachstellen zeitnah zu prüfen, während des Prozesses angemessen mit der meldenden Partei zu kommunizieren und geeignete Maßnahmen zum Schutz der Nutzer bereitzustellen.

Melden Sie mögliche Sicherheitslücken vertraulich an security@saluscontrols.com. SALUS Controls PLC bestätigt den Eingang innerhalb von drei Werktagen, spätestens jedoch nach sieben Kalendertagen. Die Bestätigung belegt nur den Eingang und bedeutet nicht, dass das gemeldete Problem als Schwachstelle bestätigt wurde.

2. Geltungsbereich

Diese Richtlinie gilt für Sicherheitslücken in:

- Produkte von SALUS Controls PLC
- Firmware und Software
- Mobile Anwendungen
- Cloud-Dienste
- Öffentlich zugänglichen Webanwendungen und Websites

Bei Fragen zu Installation, Konfiguration, Garantie oder anderen nicht sicherheitsbezogenen Themen wenden Sie sich bitte über die üblichen Supportkanäle an unser Customer-Support-Team.

Wir akzeptieren Sicherheitsmeldungen zu SALUS-Produkten unabhängig vom Lebenszyklusstatus. Innerhalb des veröffentlichten Sicherheits-Supportzeitraums werden Schwachstellen und Updates gemäß den geltenden rechtlichen Pflichten behandelt. Außerhalb dieses Zeitraums bewertet SALUS Controls PLC Meldungen weiterhin und kann je nach Risiko, technischer Machbarkeit und Pflichten Minderungsmaßnahmen, Migrationshinweise oder andere Empfehlungen geben.

3. Meldung einer Schwachstelle

Wenn Sie glauben, eine Sicherheitslücke identifiziert zu haben, melden Sie diese bitte vertraulich per E-Mail an **security@saluscontrols.com**

Meldungen können anonym erfolgen. Ein fehlender Name oder Rückkanal verhindert weder Eingang noch Erstbewertung, kann aber Rückfragen, Statusupdates oder eine öffentliche Anerkennung einschränken.

Wir akzeptieren Erstmeldungen per normaler E-Mail oder über andere Kanäle. Müssen Exploit-Code, Zugangsdaten, personenbezogene Daten, Kundenkonfigurationen oder andere sensible Informationen ausgetauscht werden, bietet SALUS Controls PLC eine verfügbare sichere Kommunikationsmethode an. Eine fehlende oder nicht genutzte Verschlüsselung führt allein nicht zur Ablehnung der Meldung.

4. Anzugebende Informationen

Für eine effiziente Prüfung geben Sie bitte nach Möglichkeit Folgendes an:

- Produktname und Modell
- Firmware- oder Softwareversion
- Beschreibung der Schwachstelle
- Schritte zur Reproduktion
- Erwartetes und tatsächliches Verhalten
- Mögliche Sicherheitsauswirkungen
- Screenshots, Logs oder Proof-of-Concept, sofern verfügbar
- Bevorzugte Kontaktdaten für Rückfragen

Vermeiden Sie sensible personenbezogene Daten, sofern sie nicht zum Nachweis der Schwachstelle erforderlich sind.

Geben Sie, soweit bekannt, auch an, ob das Problem öffentlich ist, aktiv ausgenutzt wird, Nutzer betroffen sind oder es einem anderen Lieferanten, Anbieter oder Koordinator gemeldet wurde. Nicht alle Angaben sind erforderlich, damit wir die Meldung annehmen und registrieren.

Bei koordinierter Offenlegung ist der Zugriff auf nicht öffentliche Schwachstelleninformationen auf erforderliche Personen beschränkt. SALUS Controls PLC kann notwendige Informationen mit Produktteams, Lieferanten, Koordinatoren, betroffenen Parteien oder zuständigen Behörden zur Validierung, Behebung, zum Nutzerschutz und zur Erfüllung rechtlicher Pflichten teilen, vorbehaltlich angemessener Vertraulichkeits- und Datenschutzmaßnahmen.

Personenbezogene Daten aus einer Schwachstellenmeldung werden gemäß der geltenden Datenschutzerklärung von SALUS Controls PLC verarbeitet.
Siehe:https://saluscontrols.com/de/salus-controls-gmbh-datenschutzerklaerung/

5. Reaktionsprozess

Nach Eingang Ihrer Meldung wird SALUS Controls PLC:

- Den Eingang innerhalb von drei Werktagen, spätestens nach sieben Kalendertagen, bestätigen; nach Möglichkeit mit eindeutiger Fallkennung und vorläufigem Status.
- Innerhalb von sieben Arbeitstagen eine Erstbewertung durchführen
- Die gemeldete Schwachstelle validieren
- Den Schweregrad und die möglichen Auswirkungen bewerten
- Gegebenenfalls einen Behebungsplan oder ein Sicherheitsupdate entwickeln
- Sie während Untersuchung und Behebung auf dem Laufenden halten
- Solange ein Fall aktiv ist, mindestens alle 30 Kalendertage ein inhaltliches Statusupdate geben und früher informieren, wenn sich bestätigter Umfang, Risiko, Behebungsansatz oder Offenlegungsdatum wesentlich ändern.
- Falls zusätzliche Informationen nötig sind, können wir Sie während der Untersuchung kontaktieren.

6. Risikobasierte Behebung

Bestätigte Schwachstellen werden nach technischem Schweregrad, Ausnutzbarkeit, betroffenen Produkten, möglichen Auswirkungen, Nutzerexposition, aktiver Ausnutzung, verfügbaren Minderungsmaßnahmen und sicherer Bereitstellung priorisiert. Ein numerischer Wert kann die Bewertung unterstützen, bestimmt aber nicht allein die Priorität.

SALUS Controls PLC legt ein fallspezifisches Behebungsziel fest und kommuniziert wesentliche Änderungen an die meldende Partei. Ist eine sofortige Behebung nicht möglich, können geeignete Minderungs- oder Risikoreduktionshinweise vor einer dauerhaften Lösung bereitgestellt werden.

7. Koordinierte Offenlegung von Schwachstellen

SALUS Controls PLC legt mit der meldenden Partei und bei Bedarf mit Lieferanten, Koordinatoren und Betroffenen ein fallspezifisches Offenlegungsdatum fest. Dieses kann je nach Schweregrad, aktiver Ausnutzung, Nutzerrisiko, Behebungs- und Bereitstellungsfortschritt, Lieferkettenabhängigkeiten sowie rechtlichen oder regulatorischen Pflichten angepasst werden. Wesentliche Änderungen werden mitgeteilt.

SALUS Controls PLC kann Nutzer schneller informieren oder früher öffentlich offenlegen, wenn eine Schwachstelle bereits öffentlich ist, aktiv ausgenutzt wird, ein dringendes Nutzerrisiko darstellt, wahrscheinlich bekannt wird oder eine Meldung gesetzlich vorgeschrieben ist. Ist noch keine vollständige Behebung verfügbar, kann SALUS vorübergehende Minderungs- oder Risikohinweise geben, ohne Missbrauch unnötig zu erleichtern.

Informationen zu behobenen Schwachstellen werden in zugänglichen, menschenlesbaren Sicherheitshinweisen veröffentlicht. Diese nennen Schwachstelle und betroffene Produkte, Veröffentlichungs- und Revisionsdaten, mögliche Auswirkungen und Schweregrad, verfügbare Behebungs- oder Minderungsmaßnahmen, erforderliche Nutzeraktionen und Kontaktdaten. Hinweise zu Drittkomponenten können auf maßgebliche Upstream-Informationen verweisen, damit Nutzer prüfen können, ob SALUS-Produkte betroffen sind.

Schwachstelleninformationen werden auch in einem weithin anerkannten maschinenlesbaren Format bereitgestellt, sofern eine Abweichung nicht dokumentiert und genehmigt wurde. Eine Veröffentlichung darf nur verzögert oder unterlassen werden, wenn die Bedingungen bewertet, dokumentiert und genehmigt wurden.

Soweit gesetzlich erforderlich oder zum Nutzerschutz notwendig, informiert SALUS Controls PLC betroffene Nutzer und stellt verfügbare Minderungs- oder Korrekturhinweise über geeignete zugängliche Kanäle bereit.

8. Unterstützung für Sicherheitsupdates

SALUS Controls PLC stellt während des für jedes Produkt festgelegten Supportzeitraums Sicherheitsupdates bereit. Der Zeitraum wird gemäß den geltenden gesetzlichen Anforderungen unter Berücksichtigung der erwarteten Nutzungsdauer, der Produktart und angemessener Nutzererwartungen festgelegt.

Der Supportzeitraum beträgt mindestens fünf Jahre, sofern nicht vernünftigerweise eine kürzere Nutzungsdauer zu erwarten ist, und kann bei entsprechender Produktlebensdauer länger sein. Das jeweilige Enddatum wird in den relevanten Produktinformationen mitgeteilt.

9. Außerhalb des Geltungsbereichs

Alle potenziellen Sicherheitsmeldungen werden registriert und zunächst bewertet. Rein funktionale, kommerzielle oder supportbezogene Probleme können an den passenden Supportkanal weitergeleitet werden. Kann ein Problem zunächst nicht reproduziert werden, kann SALUS Controls PLC zusätzliche Informationen anfordern und die Meldung bei neuen Nachweisen erneut bewerten.

Theoretische Probleme, physische Zugriffsszenarien, Denial-of-Service, Social Engineering und Drittanbieterabhängigkeiten werden nach realistischen Sicherheitsauswirkungen, Ausnutzbarkeit sowie der vorgesehenen und vernünftigerweise vorhersehbaren Produktnutzung bewertet.

Schwachstellen in Drittkomponenten, die in ein SALUS-Produkt integriert, mitgeliefert oder davon genutzt werden, unterliegen weiterhin der SALUS-Produktauswirkungsbewertung.

10. Verantwortungsvolle Sicherheitsforschung

SALUS Controls PLC unterstützt verantwortungsvolle Sicherheitsforschung in gutem Glauben. Wir bitten Forschende:

- Verantwortungsvoll und ethisch zu handeln
- Störungen von Produkten, Dienstleistungen oder Kundenabläufen zu vermeiden
- Zugriff, Änderung oder Löschung von Kundendaten zu vermeiden
- Schwachstellen vertraulich über den beschriebenen Prozess zu melden
- SALUS Controls PLC vor öffentlicher Offenlegung ausreichend Zeit zur Untersuchung und Behebung einzuräumen
- Alle geltenden Gesetze und Vorschriften bei der Sicherheitsforschung einzuhalten

Handelt eine meldende Partei in gutem Glauben, hält diese Richtlinie ein, vermeidet Schäden und meldet unverzüglich, beabsichtigt SALUS Controls PLC keine rechtlichen Schritte allein wegen Sicherheitsforschung nach dieser Richtlinie. Diese Erklärung erlaubt keinen Zugriff auf Systeme oder Daten Dritter, bindet keine Dritten oder Behörden und entbindet nicht von der Pflicht, geltendes Recht einzuhalten und erforderliche Genehmigungen einzuholen.

11. Kontakt

Bei allen sicherheitsbezogenen Meldungen oder Fragen zu dieser Richtlinie wenden Sie sich bitte an:

SALUS Controls PLC Security Team

E-Mail:security@saluscontrols.com

12. Aktualisierung der Richtlinie

Diese Richtlinie wird mindestens jährlich sowie nach wesentlichen Änderungen rechtlicher Anforderungen, Meldekanäle, Produktumfangs oder Schwachstellenprozesse überprüft. Aktuelle Version, Veröffentlichungsdatum, Datum der letzten Aktualisierung und Richtlinienverantwortlicher werden mit der veröffentlichten Richtlinie angezeigt.

13. Anerkennung

Mit Zustimmung der meldenden Partei kann SALUS Controls PLC Name, Alias oder Organisation einer Partei nennen, die eine gültige Schwachstellenmeldung einreicht und koordinierte Offenlegung unterstützt. Meldungen können anonym erfolgen; eine abgelehnte Anerkennung beeinflusst Annahme, Priorisierung oder Behebung nicht.

Diese Richtlinie begründet kein Bug-Bounty-Programm und garantiert keine finanziellen oder sonstigen Belohnungen.