

SALUS Controls PLC - Suspected Vulnerability Report Form

Use this form to report a suspected security vulnerability affecting a SALUS product, application, cloud service or website.

Please complete as much information as you can. You do not need to complete every field for us to accept your report.

You may submit a report anonymously. However, if you do not provide contact details, we may be unable to request additional information or provide updates about your report.

Once completed, please send this form to **security@saluscontrols.com**.

Please do not include passwords, authentication tokens, private keys or unnecessary personal/customer data.

Fields marked "Required" are required only where reasonably available. If you do not have all information, you may still submit the report.

Suspected Vulnerability Report

1. Reporter Information

Field	Response
Name or alias (Optional)	
Organisation (Optional)	
Email/Contact method (Required unless reporting anonymously)	
Preferred language (Optional)	
Reporting anonymously?	☐ Yes ☐ No

2. Affected Product or Component

Field	Response
Product or service name (Required)	
Model (If applicable)	
Hardware version (If known)	
Firmware / Software / Application version (If known)	
Country/ Region	
Other relevant configuration information	

3. Description of the Suspected Vulnerability

Field	Response
Short title (Required)	
Please describe the security issue you identified (Required)	
When did you first notice the issue?	
What did you expect to happen?	
What actually happened?	
Can you reproduce the issue?	☐ Yes ☐ No ☐ Sometimes ☐ Unknown
If possible, describe the steps needed to reproduce it:	
What security impact do you think the issue could have?	
Attachments included? You may provide relevant screenshots, logs, videos or proof-of-concept information.	☐ Yes ☐ No

Additional technical information (optional – for security researchers)

Field	Response
Vulnerability type (Authentication bypass, injection, memory corruption, etc.), if known	
CWE/ CVE, if known	
Technical cause / details	
Test environment / configuration	
Proof of concept	

4. Attack Scenario

The attack scenario is different from the reproduction procedure. Describe how a realistic attacker could exploit the issue.

Field	Response
If known, please describe how someone could exploit this vulnerability	
Attacker access	☐ Remote network ☐ Adjacent network ☐ Local network ☐ Local device ☐ Physical access ☐ Unknown
User interaction required	☐ Yes ☐ No ☐ Unknown
Special permissions/ account required	☐ Yes ☐ No ☐ Unknown If Yes, please describe the permissions / account required:

5. Impact Assessment (Optional)

Complete this section if you can assess the potential impact.

Impact area	Reporter assessment
Confidentiality	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Integrity	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Availability	☐ None ☐ Low ☒ Medium ☐ High ☐ Unknown
Safety	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Privacy	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Supply-chain or broader ecosystem impact	☐ None ☐ Low ☐ Medium ☐ High ☐ Unknown
Suggested severity, if available (Optional)	☐ Low ☐ Medium ☐ High ☐ Critical ☐ Unknown
CVSS vector, if available (Optional)	

6. Exploitation and Disclosure Status

Field	Response
Is the vulnerability already public?	☐ No ☐ Yes ☐ Unknown If yes, please provide URL and date:
Is a proof of concept public?	☐ No ☐ Yes ☐ Unknown If yes, please provide URL and date:
Is active exploitation known or suspected?	☐ No ☐ Yes ☐ Unknown If yes, please provide details:
Has another vendor, supplier, CERT or coordinator been contacted?	☐ No ☐ Yes ☐ Unknown If yes, please provide party, case ID and date:
Do you plan to discuss or publish the issue after remediation?	☐ No ☐ Yes ☐ Unknown If yes, please provide details:
Preferred coordinated disclosure date, if any	

Coordinated disclosure note:

Please keep non-public vulnerability information confidential until an agreed disclosure date. If the risk changes, active exploitation is observed, or public disclosure becomes likely, please contact security@saluscontrols.com promptly so the disclosure plan can be reassessed.

7. Suggested Remediation or Mitigation (Optional)

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

8. Acknowledgement Preference

Choice	Response
May we publicly acknowledge you if an advisory is published?	☐ Yes ☐ No
Display name, alias or organisation	
Preferred profile or reference link, if accepted by policy	

9. Attachments and Additional Information

Please list any files included with your report. Do not include passwords, authentication tokens, private keys or unnecessary personal/customer data.

Field	Response
Are files attached to this report?	☐ Yes ☐ No
Type of files attached	☐ Screenshots ☐ Logs ☐ Video ☐ Proof of concept ☐ Packet capture ☐ Other
Description of attached files	
Additional information relevant to the report	
Confidentiality or handling requirements	

If you include logs, screenshots, videos, packet captures or proof-of-concept material, please remove unnecessary personal data, customer data, passwords, authentication tokens, private keys or other sensitive information before submitting the report.

10. Good-Faith Confirmation

By submitting this report, the reporting party confirms, to the best of their knowledge, that:

- ☐ The report is accurate and was obtained through good-faith security research.
- ☐ Testing was limited to systems, devices, accounts and data the reporting party owns or was authorised to test.
- ☐ Unnecessary access to, retention of or disclosure of non-public data was avoided.
- ☐ The reporting party will coordinate disclosure in accordance with the published policy, subject to applicable law and any urgent change in user risk.
- ☐ I confirm that I have not intentionally included passwords, authentication tokens, private keys or unnecessary personal/customer data.

Submission date: _____

Reporter name or alias, if provided: _____

How to submit this report

Please email the completed form to: **security@saluscontrols.com**

You may also report a suspected vulnerability directly by email without using this form. Use of this form is recommended because it helps SALUS Controls PLC collect the information needed to assess the report efficiently.