

SALUS Controls PLC - Formulário de comunicação de suspeita de vulnerabilidade

Utilize este formulário para comunicar uma suspeita de vulnerabilidade de segurança que afete um produto, aplicação, serviço na nuvem ou website da SALUS.

Preencha o máximo de informação possível. Não é necessário preencher todos os campos para que possamos aceitar a sua comunicação.

Pode apresentar uma comunicação de forma anónima. No entanto, se não fornecer dados de contacto, poderemos não conseguir solicitar informações adicionais nem fornecer atualizações sobre a sua comunicação.

Depois de preenchido, envie este formulário para security@saluscontrols.com.

Não inclua palavras-passe, tokens de autenticação, chaves privadas nem dados pessoais/de clientes desnecessários.

Os campos assinalados como "Obrigatório" só são obrigatórios quando a informação estiver razoavelmente disponível. Mesmo que não disponha de toda a informação, pode enviar a comunicação.

Comunicação de suspeita de vulnerabilidade

1. Informações do comunicante

Campo	Resposta
Nome ou pseudónimo (Opcional)	
Organização (Opcional)	
E-mail/meio de contacto (Obrigatório, exceto em comunicações anónimas)	
Idioma preferido (Opcional)	
Comunicação anónima?	☐ Sim ☐ Não

2. Produto ou componente afetado

Campo	Resposta
Nome do produto ou serviço (Obrigatório)	
Modelo (Se aplicável)	
Versão do hardware (Se conhecida)	
Versão do firmware/software/aplicação (Se conhecida)	

Campo	Resposta
País/região	
Outras informações de configuração relevantes	

3. Descrição da suspeita de vulnerabilidade

Campo	Resposta
Título breve (Obrigatório)	
Descreva o problema de segurança identificado (Obrigatório)	
Quando detetou o problema pela primeira vez?	
O que esperava que acontecesse?	
O que aconteceu efetivamente?	
Consegue reproduzir o problema?	☐ Sim ☐ Não ☐ Às vezes ☐ Desconhecido
Se possível, descreva os passos necessários para reproduzir o problema:	
Que impacto de segurança considera que o problema poderá ter?	
Inclui anexos? Pode fornecer capturas de ecrã, registos, vídeos ou informações de prova de conceito relevantes.	☐ Sim ☐ Não

Informações técnicas adicionais (opcional – para investigadores de segurança)

Campo	Resposta
Tipo de vulnerabilidade (contorno de autenticação, injeção, corrupção de memória, etc.), se conhecido	
CWE/CVE, se conhecido	
Causa técnica/detalhes	
Ambiente de teste/configuração	
Prova de conceito	

4. Cenário de ataque

O cenário de ataque é diferente do procedimento de reprodução. Descreva como um atacante realista poderia explorar o problema.

Campo	Resposta
Se souber, descreva como alguém poderia explorar esta vulnerabilidade	
Acesso do atacante	☐ Rede remota ☐ Rede adjacente ☐ Rede local ☐ Dispositivo local ☐ Acesso físico ☐ Desconhecido
É necessária interação do utilizador	☐ Sim ☐ Não ☐ Desconhecido
São necessárias permissões especiais/conta	☐ Sim ☐ Não ☐ Desconhecido Em caso afirmativo, descreva as permissões/a conta necessárias:

5. Avaliação do impacto (Opcional)

Preencha esta secção se conseguir avaliar o impacto potencial.

Área de impacto	Avaliação do comunicante
Confidencialidade	☐ Não ☐ Baixo ☐ Médio ☐ Alto ☐ Desconhecido
Integridade	☐ Não ☐ Baixo ☐ Médio ☐ Alto ☐ Desconhecido
Disponibilidade	☐ Não ☐ Baixo ☒ Médio ☐ Alto ☐ Desconhecido
Segurança	☐ Não ☐ Baixo ☐ Médio ☐ Alto ☐ Desconhecido
Privacidade	☐ Não ☐ Baixo ☐ Médio ☐ Alto ☐ Desconhecido
Impacto na cadeia de fornecimento ou no ecossistema mais amplo	☐ Nenhum ☐ Baixo ☐ Médio ☐ Alto ☐ Desconhecido
Gravidade sugerida, se disponível (Opcional)	☐ Baixa ☐ Média ☐ Alta ☐ Crítica ☐ Desconhecida
Vetor CVSS, se disponível (Opcional)	

6. Estado de exploração e divulgação

Campo	Resposta
A vulnerabilidade já é pública?	☐ Não ☐ Sim ☐ Desconhecido Em caso afirmativo, indique o URL e a data:
Existe uma prova de conceito pública?	☐ Não ☐ Sim ☐ Desconhecido Em caso afirmativo, indique o URL e a data:
Existe exploração ativa conhecida ou suspeita?	☐ Não ☐ Sim ☐ Desconhecido Em caso afirmativo, forneça detalhes:
Foi contactado outro fabricante, fornecedor, CERT ou coordenador?	☐ Não ☐ Yes ☐ Desconhecido Em caso afirmativo, indique a entidade, o ID do caso e a data:
Pretende discutir ou publicar o problema após a correção?	☐ Não ☐ Sim ☐ Desconhecido Em caso afirmativo, forneça detalhes:
Data preferida para divulgação coordenada, se aplicável	

Nota sobre divulgação coordenada:

Mantenha confidenciais as informações não públicas sobre a vulnerabilidade até à data de divulgação acordada. Se o risco se alterar, for observada exploração ativa ou a divulgação pública se tornar provável, contacte security@saluscontrols.com rapidamente, para que o plano de divulgação possa ser reavaliado.

7. Correção ou mitigação sugerida (Opcional)

- Correção sugerida para a causa raiz, se conhecida: _____
- Mitigação temporária ou solução alternativa sugerida, se conhecida: _____
- Prática relevante do setor, regra defensiva ou referência: _____

8. Preferência de reconhecimento

Opção	Resposta
Podemos reconhecê-lo publicamente caso seja publicado um aviso de segurança?	☐ Sim ☐ Não
Nome de apresentação, pseudónimo ou organização	
Perfil ou ligação de referência preferida, se permitido pela política	

9. Anexos e informações adicionais

Liste os ficheiros incluídos com a sua comunicação. Não inclua palavras-passe, tokens de autenticação, chaves privadas nem dados pessoais/de clientes desnecessários.

Campo	Resposta
Existem ficheiros anexados a esta comunicação?	☐ Sim ☐ Não
Tipo de ficheiros anexados	☐ Capturas de ecrã ☐ Registos ☐ Vídeo ☐ Proof of concept ☐ Captura de pacotes ☐ Outro
Descrição dos ficheiros anexados	
Informações adicionais relevantes para a comunicação	
Requisitos de confidencialidade ou tratamento	

Se incluir registos, capturas de ecrã, vídeos, capturas de pacotes ou material de prova de conceito, remova dados pessoais desnecessários, dados de clientes, palavras-passe, tokens de autenticação, chaves privadas ou outras informações sensíveis antes de enviar a comunicação.

10. Confirmação de boa-fé

Ao enviar esta comunicação, o comunicante confirma, tanto quanto é do seu conhecimento, que:

- ☐ A comunicação é exata e foi obtida através de investigação de segurança realizada de boa-fé.
- ☐ Os testes limitaram-se a sistemas, dispositivos, contas e dados pertencentes ao comunicante ou para os quais tinha autorização de teste.
- ☐ Foi evitado o acesso, retenção ou divulgação desnecessários de dados não públicos.
- ☐ O comunicante coordenará a divulgação de acordo com a política publicada, sujeito à legislação aplicável e a qualquer alteração urgente do risco para os utilizadores.
- ☐ Confirmando que não incluí intencionalmente palavras-passe, tokens de autenticação, chaves privadas nem dados pessoais/de clientes desnecessários.

Data de envio: _____

Nome ou pseudónimo do comunicante, se fornecido:

Como enviar esta comunicação

Envie o formulário preenchido por e-mail para: security@saluscontrols.com

Também pode comunicar uma suspeita de vulnerabilidade diretamente por e-mail, sem utilizar este formulário. Recomenda-se a utilização deste formulário, pois ajuda a SALUS Controls PLC a recolher as informações necessárias para avaliar a comunicação de forma eficiente.