SALUS Controls PLC - Formulario de notificación de una posible vulnerabilidad

Utilice este formulario para informar de una posible vulnerabilidad de seguridad que afecte a un producto, aplicación, servicio en la nube o sitio web de SALUS.
Facilite toda la información que le sea posible. No es necesario completar todos los campos para que podamos aceptar su notificación.
Puede enviar la notificación de forma anónima. No obstante, si no facilita datos de contacto, es posible que no podamos solicitar información adicional ni comunicarle novedades sobre su notificación.
Una vez cumplimentado, envíe este formulario a security@saluscontrols.com.
No incluya contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes que no sean necesarios.
Los campos marcados como «Obligatorio» solo son obligatorios cuando la información esté razonablemente disponible. Aunque no disponga de toda la información, puede enviar la notificación.

Notificación de una posible vulnerabilidad

1. Información de la persona notificante

Campo	Respuesta
Nombre o alias (opcional)	
Organización (opcional)	
Correo electrónico / método de contacto (obligatorio salvo notificación anónima)	
Idioma preferido (opcional)	
¿Desea realizar la notificación de forma anónima?	☐ Sí ☐ No

2. Producto o componente afectado

Campo	Respuesta
Nombre del producto o servicio (obligatorio)	
Modelo (si procede)	
Versión de hardware (si se conoce)	
Versión de firmware / software / aplicación (si se conoce)	
País / región	

Campo	Respuesta
Otra información de configuración pertinente	

3. Descripción de la posible vulnerabilidad

Campo	Respuesta
Título breve (obligatorio)	
Describa el problema de seguridad identificado (obligatorio)	
¿Cuándo detectó el problema por primera vez?	
¿Qué esperaba que ocurriera?	
¿Qué ocurrió realmente?	
¿Puede reproducir el problema?	☐ Sí ☐ No ☐ A veces ☐ Desconocido
Si es posible, describa los pasos necesarios para reproducirlo:	
¿Qué impacto sobre la seguridad cree que podría tener el problema?	
¿Se incluyen archivos adjuntos? Puede aportar capturas de pantalla, registros, vídeos o información de prueba de concepto pertinentes.	☐ Sí ☐ No

Información técnica adicional (opcional, para investigadores de seguridad)

Campo	Respuesta
Tipo de vulnerabilidad (omisión de autenticación, inyección, corrupción de memoria, etc.), si se conoce	
CWE / CVE, si se conoce	
Causa técnica / detalles	
Entorno de prueba / configuración	
Prueba de concepto	

4. Escenario de ataque

El escenario de ataque es distinto del procedimiento de reproducción. Describa cómo podría un atacante realista aprovechar la vulnerabilidad.

Campo	Respuesta
Si se conoce, describa cómo podría alguien aprovechar esta vulnerabilidad	
Acceso del atacante	☐ Red remota ☐ Red adyacente ☐ Local network ☐ Local device ☐ Physical access ☐ Desconocido
Interacción del usuario necesaria	☐ Sí ☐ No ☐ Desconocido
Permisos especiales / cuenta necesarios	☐ Sí ☐ No ☐ Desconocido En caso afirmativo, describa los permisos / la cuenta necesarios:

5. Evaluación del impacto (opcional)

Complete esta sección si puede evaluar el posible impacto.

Área de impacto	Evaluación de la persona notificante
Confidencialidad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Integridad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Disponibilidad	☐ None ☐ Bajo ☒ Medio ☐ Alto ☐ Desconocido
Seguridad física	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Privacidad	☐ None ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Impacto en la cadena de suministro o en el ecosistema más amplio	☐ Ninguno ☐ Bajo ☐ Medio ☐ Alto ☐ Desconocido
Gravedad sugerida, si está disponible (opcional)	☐ Bajo ☐ Medio ☐ Alto ☐ Crítico ☐ Desconocido
Vector CVSS, si está disponible (opcional)	

6. Estado de explotación y divulgación

Campo	Respuesta
¿La vulnerabilidad ya es pública?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, indique la URL y la fecha:
¿Existe una prueba de concepto pública?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, indique la URL y la fecha:
¿Se conoce o sospecha una explotación activa?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, facilite los detalles:
¿Se ha contactado con otro fabricante, proveedor, CERT o coordinador?	☐ No ☐ Yes ☐ Desconocido En caso afirmativo, indique la entidad, el identificador del caso y la fecha:
¿Tiene previsto comentar o publicar el problema después de su corrección?	☐ No ☐ Sí ☐ Desconocido En caso afirmativo, facilite los detalles:
Fecha preferida para la divulgación coordinada, si procede	

Nota sobre divulgación coordinada:
Mantenga confidencial la información no pública sobre la vulnerabilidad hasta la fecha de divulgación acordada. Si cambia el riesgo, se observa una explotación activa o resulta probable una divulgación pública, póngase en contacto de inmediato con security@saluscontrols.com para que pueda reevaluarse el plan de divulgación.

7. Medidas correctivas o de mitigación sugeridas (opcional)

- Corrección sugerida de la causa raíz, si se conoce: _____
- Medida de mitigación temporal o solución alternativa sugerida, si se conoce: _____
- Práctica sectorial, regla defensiva o referencia pertinente: _____

8. Preferencia de reconocimiento

Opción	Respuesta
¿Podemos reconocer públicamente su contribución si se publica un aviso?	☐ Sí ☐ No
Nombre público, alias u organización	
Perfil o enlace de referencia preferido, si la política lo permite	

9. Archivos adjuntos e información adicional

Enumere los archivos incluidos con la notificación. No incluya contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes que no sean necesarios.

Campo	Respuesta
¿Hay archivos adjuntos a esta notificación?	☐ Sí ☐ No
Tipo de archivos adjuntos	☐ Capturas de pantalla ☐ Registros ☐ Vídeo ☐ Prueba de concepto ☐ Captura de paquetes ☐ Otro
Descripción de los archivos adjuntos	
Información adicional pertinente para la notificación	
Requisitos de confidencialidad o tratamiento	

Si incluye registros, capturas de pantalla, vídeos, capturas de paquetes o material de prueba de concepto, elimine antes de enviar la notificación los datos personales o de clientes innecesarios, contraseñas, tokens de autenticación, claves privadas u otra información sensible.

10. Confirmación de buena fe

Al enviar esta notificación, la persona notificante confirma, según su leal saber y entender, que:

☐ La notificación es exacta y se ha elaborado en el marco de una investigación de seguridad realizada de buena fe.
☐ Las pruebas se limitaron a sistemas, dispositivos, cuentas y datos que pertenecen a la persona notificante o para los que estaba autorizada a realizar pruebas.
☐ Se evitó el acceso, la conservación o la divulgación innecesarios de datos no públicos.
☐ La persona notificante coordinará la divulgación de conformidad con la política publicada, con sujeción a la legislación aplicable y a cualquier cambio urgente en el riesgo para los usuarios.
☐ Confirmo que no he incluido intencionadamente contraseñas, tokens de autenticación, claves privadas ni datos personales o de clientes innecesarios.

Fecha de envío: _____

Nombre o alias de la persona notificante, si se facilita:

_____

Cómo enviar esta notificación

Envíe el formulario cumplimentado por correo electrónico a: security@saluscontrols.com
También puede informar de una posible vulnerabilidad directamente por correo electrónico sin utilizar este formulario. Se recomienda utilizarlo porque ayuda a SALUS Controls PLC a recopilar la información necesaria para evaluar la notificación de forma eficiente.