SALUS Controls PLC - Formular de raportare a unei vulnerabilități suspectate

Utilizați acest formular pentru a raporta o vulnerabilitate de securitate suspectată care afectează un produs SALUS, o aplicație, un serviciu cloud sau un site web.
Vă rugăm să completați cât mai multe informații posibil. Nu este necesar să completați fiecare câmp pentru ca raportul dumneavoastră să fie acceptat.
Puteți trimite raportul în mod anonim. Totuși, dacă nu furnizați date de contact, este posibil să nu vă putem solicita informații suplimentare sau comunica actualizări privind raportul.
După completare, vă rugăm să trimiteți formularul la security@saluscontrols.com.
Vă rugăm să nu includeți parole, tokenuri de autentificare, chei private sau date personale/ale clienților care nu sunt necesare.
Câmpurile marcate „Obligatoriu" sunt obligatorii numai dacă informațiile sunt disponibile în mod rezonabil. Puteți trimite raportul chiar dacă nu dețineți toate informațiile.

Raport de vulnerabilitate suspectată

1. Date despre persoana care raportează

Informație solicitată	Răspuns
Nume sau alias (Opțional)	
Organizație (Opțional)	
E-mail / metodă de contact (Obligatoriu, cu excepția raportării anonime)	
Limba preferată (Opțional)	
Raportați anonim?	☐ Da ☐ Nu

2. Produsul sau componenta afectată

Informație solicitată	Răspuns
Numele produsului sau serviciului (Obligatoriu)	
Model (Dacă este cazul)	
Versiune hardware (Dacă este cunoscută)	
Versiune firmware / software / aplicație (Dacă este cunoscută)	
Țară / regiune	
Alte informații relevante despre configurație	

3. Descrierea vulnerabilității suspectate

Informație solicitată	Răspuns
Titlu scurt (Obligatoriu)	
Descrieți problema de securitate identificată (Obligatoriu)	
Când ați observat prima dată problema?	
Ce vă așteptați să se întâmple?	
Ce s-a întâmplat în realitate?	
Puteți reproduce problema?	☐ Da ☐ Nu ☐ Uneori ☐ Necunoscut
Dacă este posibil, descrieți pașii necesari pentru reproducerea problemei:	
Ce impact asupra securității considerați că ar putea avea problema?	
Sunt incluse fișiere atașate? Puteți furniza capturi de ecran, jurnale, materiale video sau informații proof-of-concept relevante.	☐ Da ☐ Nu

Informații tehnice suplimentare (opțional – pentru cercetători în securitate)

Informație solicitată	Răspuns
Tipul vulnerabilității (ocolirea autentificării, injecție, coruperea memoriei etc.), dacă este cunoscut	
CWE/CVE, dacă este cunoscut	
Cauza tehnică / detalii	
Mediu de testare / configurație	
Proof of concept	

4. Scenariul de atac

Scenariul de atac diferă de pașii de reproducere. Descrieți cum ar putea un atacator să exploateze vulnerabilitatea în mod realist.

Informație solicitată	Răspuns
Dacă este cunoscut, descrieți modul în care cineva ar putea exploata această vulnerabilitate	
Acces necesar atacatorului	☐ Rețea la distanță ☐ Rețea adiacentă ☐ Rețea locală ☐ Dispozitiv local ☐ Acces fizic ☐ Necunoscut
Este necesară interacțiunea utilizatorului?	☐ Da ☐ Nu ☐ Necunoscut
Sunt necesare permisiuni speciale / un cont?	☐ Da ☐ Nu ☐ Necunoscut Dacă da, descrieți permisiunile / contul necesar:

5. Evaluarea impactului (Opțional)

Completați această secțiune dacă puteți evalua impactul potențial.

Domeniul impactului	Evaluarea persoanei care raportează
Confidențialitate	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Integritate	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Disponibilitate	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Siguranță	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Viață privată	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Impact asupra lanțului de aprovizionare sau ecosistemului	☐ Niciunul ☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Necunoscut
Severitate sugerată, dacă poate fi evaluată (Opțional)	☐ Scăzut ☐ Mediu ☐ Ridicat ☐ Critic ☐ Necunoscut
Vector CVSS, dacă este disponibil (Opțional)	

6. Stadiul exploatării și dezvăluirii

Informație solicitată	Răspuns
Vulnerabilitatea este deja publică?	☐ Nu ☐ Da ☐ Necunoscut Dacă da, furnizați URL-ul și data:
Există o dovadă de concept (PoC) publică?	☐ Nu ☐ Da ☐ Necunoscut Dacă da, furnizați URL-ul și data:
Este cunoscută sau suspectată exploatarea activă?	☐ Nu ☐ Da ☐ Necunoscut Dacă da, furnizați detalii:
A fost contactat un alt producător, furnizor, CERT sau coordonator?	☐ Nu ☐ Da☐ Necunoscut Dacă da, indicați partea contactată, ID-ul cazului și data:
Intenționați să discutați sau să publicați problema după remediere?	☐ Nu ☐ Da ☐ Necunoscut Dacă da, furnizați detalii:
Data preferată pentru dezvăluirea coordonată, dacă există	

Notă privind dezvăluirea coordonată:
Vă rugăm să păstrați confidențiale informațiile nepublice despre vulnerabilitate până la data convenită pentru dezvăluire. Dacă nivelul de risc se modifică, se observă o exploatare activă sau dezvăluirea publică devine probabilă, contactați prompt **security@saluscontrols.com** pentru reevaluarea planului de dezvăluire.

7. Remediere sau măsuri de atenuare sugerate (Opțional)

- Remediere sugerată a cauzei principale, dacă este cunoscută: _____
- Măsură temporară de atenuare sau soluție alternativă sugerată, dacă este cunoscută:_____
- Practică relevantă din industrie, regulă defensivă sau referință: _____

8. Preferință privind recunoașterea publică

Opțiune	Răspuns
Vă putem menționa public dacă este publicat un aviz de securitate?	☐ Da ☐ Nu
Nume afișat, alias sau organizație	
Profil preferat sau link de referință, dacă este acceptat de politică	

9. Fișiere atașate și informații suplimentare

Vă rugăm să enumerați fișierele incluse în raport. Nu includeți parole, tokenuri de autentificare, chei private sau date personale/ale clienților care nu sunt necesare.

Informație solicitată	Răspuns
Sunt atașate fișiere la acest raport?	☐ Da ☐ Nu
Tipul fișierelor atașate	☐ Capturi de ecran ☐ Jurnale ☐ Video ☐ Proof of concept ☐ Captură de pachete de rețea ☐ Altele
Descrierea fișierelor atașate	
Informații suplimentare relevante pentru raport	
Cerințe de confidențialitate sau manipulare	

Dacă includeți jurnale, capturi de ecran, materiale video, capturi de pachete sau materiale demonstrative (proof-of-concept), eliminați înainte de trimiterea raportului datele personale sau ale clienților care nu sunt necesare, parolele, tokenurile de autentificare, cheile private ori alte informații sensibile.

10. Confirmare de bună-credință

Prin trimiterea acestui raport, persoana care raportează confirmă, după cunoștințele sale, că:

☐ Raportul este corect, iar informațiile au fost obținute prin cercetare de securitate efectuată cu bună-credință.

☐ Testarea s-a limitat la sisteme, dispozitive, conturi și date deținute de persoana care raportează sau pentru care aceasta a fost autorizată să efectueze teste.

☐ A fost evitat accesul inutil la date nepublice, păstrarea acestora sau divulgarea lor.

☐ Persoana care raportează va coordona divulgarea în conformitate cu politica publicată, cu respectarea legislației aplicabile și a oricărei modificări urgente a riscului pentru utilizatori.

☐ Confirm că nu am inclus în mod intenționat parole, tokenuri de autentificare, chei private sau date personale/ale clienților care nu sunt necesare.

Data trimiterii: _____

Numele sau aliasul persoanei care raportează, dacă este furnizat:

_____

Cum se trimite acest raport

Vă rugăm să trimiteți formularul completat prin e-mail la: security@saluscontrols.com
De asemenea, puteți raporta o vulnerabilitate suspectată direct prin e-mail, fără a utiliza acest formular.
Utilizarea formularului este recomandată deoarece ajută SALUS Controls PLC să colecteze informațiile necesare pentru evaluarea eficientă a raportului.