Politica de divulgare a vulnerabilităților

Raportarea responsabilă, investigarea și remedierea vulnerabilităților de securitate

Versiune	Data intrării în vigoare	Responsabil document	Contact
1.0	Septembrie 2026	Echipa de securitate SALUS Controls PLC	security@saluscontrols.com

1. Introducere 2
2. Domeniu de aplicare 2
3. Raportarea unei vulnerabilități 2
4. Informații de inclus 3
5. Procesul de răspuns 3
6. Remedierea în funcție de risc 4
7. Divulgarea coordonată a vulnerabilităților 4
8. Suport pentru actualizări de securitate 4
9. În afara domeniului de aplicare 5
10. Cercetare responsabilă în domeniul securității 5
11. Contact 5
12. Actualizări ale politicii 6
13. Recunoaștere 6

1. Introducere

SALUS Controls PLC se angajează să protejeze securitatea produselor, serviciilor și clienților săi. Încurajăm raportările responsabile din partea clienților, cercetătorilor în securitate, partenerilor, dezvoltatorilor și altor membri ai comunității de securitate care identifică potențiale vulnerabilități ce afectează produsele sau serviciile SALUS Controls PLC.

Obiectivul nostru este să investigăm prompt raportările privind potențiale vulnerabilități, să comunicăm corespunzător cu persoana care raportează pe tot parcursul procesului și să oferim măsuri proporționale de remediere sau reducere a riscului pentru protejarea utilizatorilor.

Raportați în mod privat potențialele vulnerabilități de securitate la **security@saluscontrols.com**. SALUS Controls PLC va confirma primirea în termen de trei zile lucrătoare și, în toate cazurile, nu mai târziu de șapte zile calendaristice. Această confirmare doar atestă primirea informațiilor și nu înseamnă că problema raportată a fost confirmată drept vulnerabilitate.

2. Domeniu de aplicare

Această politică se aplică vulnerabilităților de securitate care afectează:

- Produsele SALUS Controls PLC
- Firmware și software
- Aplicații mobile
- Servicii cloud
- Aplicații web și site-uri accesibile publicului

Pentru întrebări privind instalarea, configurarea, garanția produselor sau alte aspecte fără legătură cu securitatea, vă rugăm să contactați echipa noastră de Asistență Clienți prin canalele standard de suport.

Acceptăm raportări de securitate privind produsele SALUS indiferent de stadiul ciclului lor de viață. Pentru produsele aflate în perioada publicată de suport de securitate, vulnerabilitățile și actualizările de securitate sunt gestionate conform obligațiilor legale aplicabile. Pentru produsele din afara acestei perioade, SALUS Controls PLC va evalua în continuare raportările și poate oferi măsuri de reducere a riscului, recomandări de migrare sau alte îndrumări, în funcție de risc, fezabilitatea tehnică și obligațiile aplicabile.

3. Raportarea unei vulnerabilități

Dacă considerați că ați identificat o vulnerabilitate de securitate, vă rugăm să o raportați în mod privat prin e-mail la **security@saluscontrols.com**. Vă rugăm să raportați vulnerabilitățile suspectate folosind acest **șablon**.

Raportările pot fi transmise anonim. Lipsa unui nume sau a unei metode de contact bidirecționale nu va împiedica primirea ori evaluarea inițială, dar ne poate limita posibilitatea de a solicita informații suplimentare, de a furniza actualizări de stare sau de a oferi recunoaștere publică.

Acceptăm un raport inițial trimis prin e-mail obișnuit sau prin alt canal. Dacă trebuie schimbate cod de exploatare, date de autentificare, date cu caracter personal, configurații ale clienților sau alte informații sensibile, SALUS Controls PLC va pune la dispoziție o metodă sigură disponibilă pentru continuarea comunicării. Imposibilitatea sau decizia persoanei care raportează de a nu utiliza criptarea nu va determina, în sine, respingerea raportului.

4. Informații de inclus

Pentru a ne ajuta să investigăm eficient raportarea, vă rugăm să includeți, acolo unde este posibil:

- Denumirea și modelul produsului
- Versiunea de firmware sau software
- Descrierea vulnerabilității
- Pașii necesari pentru reproducerea problemei
- Comportamentul așteptat și cel real
- Impactul potențial asupra securității
- Capturi de ecran, jurnale sau dovadă de concept, dacă sunt disponibile
- Datele de contact preferate pentru comunicări ulterioare

Vă rugăm să evitați includerea informațiilor personale sensibile, cu excepția cazului în care acestea sunt necesare pentru a demonstra vulnerabilitatea.

De asemenea, indicați, dacă știți, dacă problema este publică, este exploatată activ, a afectat utilizatori sau a fost raportată unui alt furnizor, comerciant sau coordonator. Nu este necesar să furnizați toate elementele solicitate pentru ca noi să acceptăm și să înregistrăm raportarea.

În cadrul divulgării coordonate, accesul la informațiile nepublice despre vulnerabilități este limitat pe principiul necesității de a cunoaște. SALUS Controls PLC poate partaja informațiile necesare cu echipele de produs, furnizorii, coordonatorii, părțile afectate sau autoritățile competente pentru validare, remediere, protejarea utilizatorilor și respectarea obligațiilor legale, sub rezerva unor măsuri adecvate de confidențialitate și protecție a datelor.

Datele cu caracter personal transmise împreună cu o raportare de vulnerabilitate sunt prelucrate în conformitate cu politica de confidențialitate aplicabilă a SALUS Controls PLC. Consultați politica de confidențialitate: https://saluscontrols.com/ro/protectia-si-confidentialitatea-datelor/.

5. Procesul de răspuns

După primirea raportării, SALUS Controls PLC va:

- Confirma primirea în termen de trei zile lucrătoare și, în toate cazurile, nu mai târziu de șapte zile calendaristice; acolo unde este posibil, va include un identificator unic al cazului și informații preliminare privind starea acestuia.
- Efectua o evaluare inițială în termen de șapte zile lucrătoare
- Valida vulnerabilitatea raportată
- Evalua gravitatea și impactul potențial
- Elabora un plan de remediere sau o actualizare de securitate, după caz
- Vă ține la curent pe parcursul procesului de investigare și remediere
- Cât timp un caz rămâne activ, va furniza o actualizare relevantă privind starea cel puțin o dată la 30 de zile calendaristice și va comunica mai devreme atunci când domeniul confirmat, riscul, abordarea de remediere sau data divulgării se modifică semnificativ.
- Dacă sunt necesare informații suplimentare, vă putem contacta pe parcursul investigației.

6. Remedierea în funcție de risc

Vulnerabilitățile confirmate sunt prioritizate în funcție de gravitatea tehnică, posibilitatea de exploatare, produsele afectate, impactul potențial, expunerea utilizatorilor, dovezile de exploatare activă, măsurile de reducere a riscului disponibile și necesitățile unei implementări sigure. Un scor numeric poate contribui la evaluare, dar nu determină singur prioritatea remedierii.

SALUS Controls PLC stabilește pentru fiecare caz un obiectiv de remediere și comunică persoanei care a raportat orice modificări semnificative. Atunci când remedierea imediată nu este posibilă, pot fi furnizate măsuri adecvate de reducere a riscului sau îndrumări înainte ca o soluție permanentă să fie disponibilă.

7. Divulgarea coordonată a vulnerabilităților

SALUS Controls PLC colaborează cu persoana care raportează și, când este necesar, cu furnizorii, coordonatorii și alte părți afectate pentru a stabili o dată de divulgare specifică fiecărui caz. Calendarul poate fi revizuit în funcție de gravitate, exploatarea activă, riscul pentru utilizatori, progresul remedierii și implementării, dependențele din lanțul de aprovizionare și obligațiile legale sau de reglementare aplicabile. Modificările semnificative ale datei țintă vor fi comunicate părților relevante.

SALUS Controls PLC poate accelera notificarea utilizatorilor sau divulgarea publică atunci când o vulnerabilitate este deja publică, este exploatată activ, prezintă un risc urgent pentru utilizatori, este probabil să devină publică sau când notificarea este impusă de lege. Dacă o remediere completă nu este încă disponibilă, SALUS poate oferi măsuri temporare de reducere a riscului sau îndrumări fără a facilita inutil exploatarea.

Informațiile despre vulnerabilitățile remediate vor fi publicate în avize de securitate accesibile și ușor de înțeles. Acestea vor identifica vulnerabilitatea și produsele afectate, datele publicării și revizuirii, impactul și gravitatea potențială, măsurile de remediere sau reducere a riscului

disponibile, acțiunile necesare din partea utilizatorilor și informațiile de contact. Avizele privind componente terțe pot face trimitere la informații autorizate din sursa originală atunci când acest lucru permite utilizatorilor să stabilească dacă produsele SALUS sunt afectate.

Informațiile despre vulnerabilități vor fi puse la dispoziție și într-un format recunoscut pe scară largă lizibil automat, cu excepția cazului în care este documentată și aprobată o justificare pentru nepublicarea în acest format. Publicarea poate fi amânată sau omisă numai dacă au fost evaluate, documentate și aprobate condițiile aplicabile.

Atunci când legea aplicabilă o impune sau este necesar pentru protejarea utilizatorilor, SALUS Controls PLC va informa utilizatorii afectați și va furniza prin canale accesibile adecvate măsurile de reducere a riscului sau îndrumările corective disponibile.

8. Suport pentru actualizări de securitate

SALUS Controls PLC furnizează actualizări de securitate pe întreaga perioadă de suport stabilită pentru fiecare produs aplicabil. Perioada de suport este determinată în conformitate cu cerințele legale aplicabile, ținând cont de durata estimată de utilizare a produsului, natura acestuia și așteptările rezonabile ale utilizatorilor.

Perioada de suport va fi de cel puțin cinci ani, cu excepția cazului în care se estimează în mod rezonabil că produsul va fi utilizat pentru o perioadă mai scurtă, și poate fi mai lungă dacă acest lucru este justificat de durata de viață estimată a produsului. Data de încheiere a perioadei de suport aplicabile va fi comunicată prin informațiile relevante despre produs.

9. În afara domeniului de aplicare

Toate potențialele raportări de securitate sunt înregistrate și primesc o evaluare inițială. Problemele exclusiv funcționale, comerciale sau legate de suport pot fi direcționate către canalul de asistență corespunzător. Dacă o problemă nu poate fi reprodusă inițial, SALUS Controls PLC poate solicita informații suplimentare și poate reevalua raportarea atunci când apar dovezi noi.

Problemele teoretice, scenariile care presupun acces fizic, condițiile de tip refuz al serviciului, scenariile de inginerie socială și dependențele de terți sunt evaluate în funcție de impactul realist asupra securității, posibilitatea de exploatare și utilizarea prevăzută și rezonabil previzibilă a produsului.

Vulnerabilitățile din componente terțe integrate într-un produs SALUS, furnizate împreună cu acesta sau de care acesta depinde rămân supuse evaluării impactului asupra produsului SALUS.

10. Cercetare responsabilă în domeniul securității

SALUS Controls PLC sprijină cercetarea responsabilă în domeniul securității, desfășurată cu bună-credință. Solicităm cercetătorilor să:

- Acționeze responsabil și etic
- Evite perturbarea produselor, serviciilor sau operațiunilor clienților
- Evite accesarea, modificarea sau ștergerea datelor clienților

- Raporteze vulnerabilitățile în mod privat, prin procesul descris în această politică
- Acorde SALUS Controls PLC un interval rezonabil pentru investigarea și remedierea problemei înainte de divulgarea publică
- Respecte toate legile și reglementările aplicabile în timpul cercetării de securitate

Atunci când persoana care raportează acționează cu bună-credință, respectă această politică, evită producerea de prejudicii și raportează prompt, SALUS Controls PLC nu intenționează să inițieze acțiuni în justiție exclusiv din cauza cercetării de securitate desfășurate în conformitate cu această politică. Această declarație nu autorizează accesul la sisteme sau date ale terților, nu obligă terți sau autorități și nu elimină obligația persoanei care raportează de a respecta legislația aplicabilă și de a obține permisiunile necesare.

11. Contact

Pentru toate raportările legate de securitate sau întrebările privind această politică, vă rugăm să contactați:

Echipa de securitate SALUS Controls PLC

E-mail: **security@saluscontrols.com**

12. Actualizări ale politicii

Această politică este revizuită cel puțin anual și după modificări semnificative ale cerințelor legale aplicabile, canalelor de raportare, domeniului produselor sau proceselor de gestionare a vulnerabilităților. Versiunea curentă, data publicării, data ultimei actualizări și responsabilul politicii sunt afișate împreună cu politica publicată.

13. Recunoaștere

Cu acordul persoanei care raportează, SALUS Controls PLC poate menționa numele, pseudonimul sau organizația unei persoane care transmite o raportare validă de vulnerabilitate și sprijină divulgarea coordonată. Raportările pot fi transmise anonim, iar refuzul recunoașterii publice nu afectează acceptarea, prioritizarea sau deciziile de remediere.

Această politică nu instituie un program de recompense pentru vulnerabilități și nu garantează recompense financiare sau de altă natură.

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.