Politica di Divulgazione Coordinata delle Vulnerabilità

Coordinated Vulnerability Disclosure (CVD) · Prodotto LineStrategy

Regolamento (UE) 2024/2847 (Cyber Resilience Act) — art. 13, par. 17 (punto di contatto unico)

Documento controllato

• • •

Dati Documento

Documento	Politica di Divulgazione Coordinata delle Vulnerabilità (CVD)
Organizzazione	Nimax S.p.A.
Tipo documento	Policy
Versione	1.0.1
Data di entrata in vigore	17/09/2026
Ultima revisione	20/10/2026
Prossima revisione	entro 12 mesi
Proprietario del documento	IT Security
Contatto	cybersecurity@nimax.it
Classificazione	Documento controllato

Sommario

1. Perché questa policy 2
2. Ambito di applicazione 2
3. Come segnalare una vulnerabilità 3
4. Cosa facciamo noi: i nostri impegni 4
5. Classificazione e tempi di correzione 4
6. Divulgazione coordinata 5
7. Tutela di chi segnala (safe harbour) 5
8. Ricompense 5
9. Trattamento dei dati personali 5
10. Escalation 6

1. Perché questa policy

La sicurezza dei prodotti software che sviluppiamo è parte della loro qualità. Nessun software è privo di difetti: quello che conta è quanto rapidamente e in modo trasparente li individuiamo e li correggiamo.

Nimax S.p.A. accoglie con favore le segnalazioni di vulnerabilità di sicurezza da parte di ricercatori indipendenti, clienti, partner e fornitori. Questo documento descrive come segnalarci una vulnerabilità, cosa facciamo quando la riceviamo e quali impegni reciproci ci assumiamo.

Questa policy attua gli obblighi previsti dal Regolamento (UE) 2024/2847 (Cyber Resilience Act) — in particolare l'art. 13, par. 17 (punto di contatto unico) e l'Allegato I, Parte II, punti 5 e 6 (politica di divulgazione coordinata e indirizzo di contatto per la segnalazione) — ed è ispirata alle norme ISO/IEC 29147 (divulgazione delle vulnerabilità) e ISO/IEC 30111 (gestione e risoluzione delle vulnerabilità).

Le relative decorrenze sono distinte: gli obblighi sul punto di contatto unico e sulla politica di divulgazione coordinata (art. 13, par. 17, e Allegato I, Parte II, punti 5 e 6) si applicano dall'11 dicembre 2027 e la presente policy ne anticipa volontariamente l'attuazione; gli obblighi di notifica di cui all'art. 14 sono invece già applicabili dall'11 settembre 2026 e riguardano, ricorrendone i presupposti, anche i prodotti già immessi sul mercato.

La presente policy è redatta in italiano; in caso di discrepanza con eventuali traduzioni (ad esempio in inglese), prevale la versione italiana.

2. Ambito di applicazione

2.1 Prodotti e servizi inclusi

Prodotto	Ambito
LineStrategy	Tutte le versioni attualmente supportate, inclusi componenti server, client, interfacce di integrazione e servizi cloud associati

Nel perimetro rientrano anche i domini e i sistemi pubblici direttamente utilizzati per l'erogazione o la distribuzione di LineStrategy.

Le attività di ricerca sono autorizzate esclusivamente sugli ambienti che Nimax ha titolo ad autorizzare; sono escluse le installazioni e i sistemi dei clienti presso cui LineStrategy è installato, nonché i sistemi di terzi.

Questo elenco viene aggiornato ogni volta che un nuovo prodotto Nimax entra nel perimetro del programma. Fa fede la versione pubblicata su questa pagina.

2.2 Fuori ambito

Sono esclusi da questa policy:

- prodotti di terze parti distribuiti o rivenduti da Nimax, per i quali la segnalazione va indirizzata al rispettivo fabbricante (se ci contattate comunque, faremo da tramite);
- siti web istituzionali e di marketing non collegati a LineStrategy;
- segnalazioni che non descrivono un impatto concreto sulla sicurezza, in particolare:
  - output di scanner automatici privo di verifica manuale e di dimostrazione di sfruttabilità;
  - assenza di header HTTP di sicurezza "best practice" senza un vettore di attacco dimostrabile;
  - questioni di configurazione TLS o supporto di cifrari legacy senza exploit pratico;
  - enumerazione di utenze, rate limiting, self-XSS, clickjacking su pagine non sensibili;
  - vulnerabilità che richiedono accesso fisico non autorizzato al dispositivo dell'utente, o un dispositivo già compromesso;
  - vulnerabilità in versioni di LineStrategy non più supportate.

2.3 Attività non consentite

Nel condurre le vostre attività di ricerca non dovete:

- accedere, modificare, esfiltrare o distruggere dati che non vi appartengono;
- degradare la disponibilità del servizio (test di denial of service, stress test, fuzzing su ambienti di produzione);
- utilizzare tecniche di ingegneria sociale, phishing o pretexting verso dipendenti, clienti o fornitori Nimax;
- attaccare fisicamente le sedi o le infrastrutture Nimax;
- installare backdoor, malware o meccanismi di persistenza;
- utilizzare la vulnerabilità oltre il minimo indispensabile a dimostrarne l'esistenza.

Se durante la ricerca vi imbattete accidentalmente in dati personali o riservati, interrompete immediatamente l'attività, non copiateli e segnalatecelo.

3. Come segnalare una vulnerabilità

3.1 Canale

Email: cybersecurity@nimax.it

Questa casella è presidiata da personale Nimax nei giorni lavorativi. È il punto di contatto unico ai sensi dell'art. 13, par. 17 del Cyber Resilience Act.

Se ritenete che i dettagli tecnici o il proof of concept siano troppo sensibili per essere inviati via email in chiaro, scriveteci senza allegarli: concorderemo con voi un canale sicuro per trasmetterli.

Accettiamo segnalazioni in italiano e in inglese. Accettiamo segnalazioni anonime: non è necessario identificarsi, anche se un canale di contatto ci permette di chiedervi chiarimenti e di tenervi aggiornati.

Il nostro contatto è pubblicato anche in formato machine-readable secondo lo standard RFC 9116, all'indirizzo https://www.nimax.it/.well-known/security.txt

3.2 Cosa includere nella segnalazione

Più la segnalazione è completa, più velocemente possiamo correggere. Vi chiediamo, se possibile:

1. Prodotto e versione interessati (es. LineStrategy 4.2.1) e ambiente in cui avete riprodotto il problema;
2. Tipo di vulnerabilità (es. SQL injection, escalation di privilegi, esposizione di dati);
3. Passi per riprodurre, il più dettagliati possibile;

4. Impatto: cosa può ottenere un attaccante che sfrutti il problema;
5. Prerequisiti: serve autenticazione? quale ruolo? serve accesso alla rete interna?
6. Materiale di supporto: screenshot, log, proof of concept, codice;
7. Se applicabile, un identificativo CVE già assegnato;
8. Come volete essere accreditati (nome, handle, organizzazione) oppure se preferite restare anonimi;
9. Se avete un vincolo di pubblicazione (conferenza, articolo) con una data già fissata.

4. Cosa facciamo noi: i nostri impegni

I tempi e gli impegni indicati nel presente documento costituiscono obiettivi di servizio: non sono garantiti, non costituiscono livelli di servizio (SLA) contrattuali né diritti di terzi, e restano salvi i termini obbligatori di legge.

Fase	Impegno Nimax
Presa in carico	Confermiamo la ricezione entro 2 giorni lavorativi
Prima valutazione	Vi comunichiamo l'esito della triage — vulnerabilità confermata, non riproducibile, fuori ambito o duplicato — entro 10 giorni lavorativi
Aggiornamenti	Vi teniamo informati almeno ogni 30 giorni fino alla chiusura
Correzione	Correggiamo in funzione della gravità (vedi §5)
Pubblicazione	Pubblichiamo un security advisory secondo il criterio del §6 (alla prima tra: disponibilità della correzione, scadenza dei 90 giorni, data concordata).
Riconoscimento	Vi citiamo nell'advisory e nella nostra pagina di ringraziamenti, se lo desiderate

Inoltre:

- Non vi chiediamo di firmare un accordo di riservatezza come condizione per segnalare.
- Non vi chiediamo di rinunciare al vostro diritto di pubblicare, una volta trascorso il periodo concordato.
- Se non siamo d'accordo con la vostra valutazione di gravità, ve lo diciamo e vi spieghiamo perché.

5. Classificazione e tempi di correzione

Valutiamo la gravità con CVSS v4.0, integrata con il contesto d'uso reale di LineStrategy. I tempi indicati decorrono dalla conferma della vulnerabilità e rappresentano il nostro obiettivo di servizio.

La presa in carico e la prima valutazione (triage) decorrono dalla data di ricezione della segnalazione sul canale di cui al §3.1. I termini sono calcolati in giorni lavorativi, salvo diversa indicazione, e possono essere sospesi in attesa delle informazioni necessarie dal segnalante. I termini costituiscono obiettivi operativi e non obbligazioni contrattuali.

Gravità	CVSS	Obiettivo di correzione
Critica	9.0 – 10.0	15 giorni solari
Alta	7.0 – 8.9	30 giorni solari
Media	4.0 – 6.9	90 giorni solari
Bassa	0.1 – 3.9	prossima release pianificata

Per le vulnerabilità critiche o attivamente sfruttate possiamo rilasciare una mitigazione temporanea o una patch fuori ciclo.

Qualora una vulnerabilità di LineStrategy risulti attivamente sfruttata, oppure si verifichi un incidente grave che incide sulla sicurezza del prodotto, Nimax procede alle notifiche verso il CSIRT competente e l'ENISA nei termini e con le modalità previsti dall'art. 14 del Cyber Resilience Act. Tali obblighi di notifica sono in capo a Nimax in qualità di fabbricante, non

ricadono sul segnalante e sono adempiuti secondo i termini di legge, i quali prevalgono sui tempi di risposta al segnalante indicati nella presente policy.

6. Divulgazione coordinata

- Il termine standard di divulgazione è di 90 giorni solari dalla conferma della vulnerabilità. Tale termine è un obiettivo, modulato in funzione del rischio e delle misure di mitigazione disponibili; restano fermi i termini obbligatori di legge e gli obblighi di notifica di cui al §5.
- Pubblichiamo l'advisory alla prima tra: la disponibilità della correzione, la scadenza dei 90 giorni, o la data concordata con voi.
- Se la correzione richiede più tempo (ad esempio per una dipendenza di terze parti o per un impatto architetturale), ve lo comunichiamo prima della scadenza e concordiamo insieme una nuova data.
- Se la vulnerabilità viene resa pubblica da terzi o risulta attivamente sfruttata, possiamo anticipare la pubblicazione per proteggere gli utenti.
- Vi chiediamo di non divulgare i dettagli prima della data concordata.
- Richiediamo un identificativo CVE per le vulnerabilità confermate che riguardano versioni già rilasciate.

I nostri security advisory sono pubblicati su: https://www.nimax.it/security/advisories

7. Tutela di chi segnala (safe harbour)

Se conducete la vostra ricerca in buona fede, nel rispetto di questa policy e sugli ambienti che Nimax ha titolo ad autorizzare, Nimax S.p.A. si impegna a:

- non avviare né sostenere azioni legali nei vostri confronti, civili o penali, in relazione alla vostra attività di ricerca, fatti salvi gli obblighi di legge, le richieste delle autorità competenti e i diritti dei terzi;
- non segnalare spontaneamente la vostra attività di ricerca alle autorità, fermi restando gli obblighi di legge e gli eventuali obblighi di comunicazione o collaborazione nei confronti delle autorità competenti;
- considerare la vostra attività come autorizzata limitatamente agli ambienti che Nimax ha titolo ad autorizzare e nei limiti delle condizioni di licenza d'uso di LineStrategy; l'autorizzazione non si estende alle installazioni e ai sistemi dei clienti né a sistemi di terzi;
- sostenervi, nei limiti del possibile, qualora un terzo intraprendesse azioni nei vostri confronti per un'attività svolta nel rispetto di questa policy.

Questa tutela non si estende ad attività condotte in violazione del §2.3, ad attività a scopo di estorsione, ad attività su sistemi di terzi o sulle installazioni e sui sistemi dei clienti.

Se avete dubbi sul fatto che una specifica attività rientri in questa policy, chiedeteci prima a cybersecurity@nimax.it.

8. Ricompense

Nimax S.p.A. non gestisce attualmente un programma di bug bounty e non corrisponde ricompense economiche per le segnalazioni.

Riconosciamo il contributo dei ricercatori attraverso la citazione nei security advisory e nella pagina di ringraziamenti, previo loro consenso.

9. Trattamento dei dati personali

I dati personali conferiti o comunque trattati nell'ambito della gestione delle segnalazioni sono trattati da Nimax S.p.A. in qualità di titolare del trattamento, secondo quanto segue.

Finalità: gestione e riscontro delle segnalazioni di vulnerabilità; adempimento degli obblighi di notifica e di documentazione previsti dal Cyber Resilience Act; eventuale accreditamento pubblico del segnalante, previo suo consenso.

Basi giuridiche: per la gestione della segnalazione e la sicurezza dei prodotti, il legittimo interesse del titolare (art. 6, par. 1, lett. f, GDPR), previa valutazione di bilanciamento; per gli

adempimenti di notifica e documentazione, l'adempimento di un obbligo legale (art. 6, par. 1, lett. c, GDPR).

Dati trattati: i dati di contatto forniti dal segnalante e i dati eventualmente contenuti nella segnalazione. Anche in caso di segnalazione anonima possono essere trattati dati personali presenti, ad esempio, in log, metadati, indirizzi IP e allegati.

Destinatari: personale autorizzato di Nimax (IT Security / CSIRT), eventuali fornitori che operano come responsabili del trattamento e, ove previsto dalla legge, le autorità competenti (CSIRT / ENISA).

Conservazione: per il tempo necessario alla gestione della segnalazione e, successivamente, per i termini previsti dagli obblighi di documentazione del Cyber Resilience Act; i criteri e i tempi determinati di conservazione sono definiti con il Referente Privacy/DPO.

Diritti degli interessati e contatti: i diritti esercitabili e i riferimenti del titolare e del Responsabile della protezione dei dati sono indicati nell'informativa privacy di Nimax, che la presente sezione integra per lo specifico trattamento.

Informativa privacy generale (integrata dalla presente sezione): https://www.nimax.it/privacy

10. Escalation

Se non ricevete risposta entro i termini indicati al §4, o se ritenete che la vostra segnalazione non sia stata gestita adeguatamente, potete:

1. contattare la Direzione IT di Nimax (IT Manager) scrivendo a cybersecurity@nimax.it e indicando nell'oggetto «Escalation»;
2. rivolgervi al CSIRT Italia (Agenzia per la Cybersicurezza Nazionale), che opera come intermediario fiduciario nel quadro della divulgazione coordinata previsto dall'art. 12 della Direttiva (UE) 2022/2555 — https://www.acn.gov.it/portale/csirt-italia