Politica di sicurezza e divulgazione delle vulnerabilità

Il **Cyber Resilience Act (CRA)** è un regolamento fondamentale dell'Unione Europea che stabilisce requisiti di cybersecurity obbligatori per i prodotti hardware e software con elementi digitali immessi sul mercato UE. Affrontando le vulnerabilità lungo l'intero ciclo di vita del prodotto, il CRA mira a proteggere consumatori e aziende dalle minacce informatiche, garantendo che “security by design” diventi lo standard di base per i dispositivi connessi.

Pilastri chiave del CRA:

Voce
Security by Design & Default: I prodotti devono essere sviluppati e consegnati con configurazioni di sicurezza ottimali, riducendo al minimo la superficie di attacco sin dal primo giorno.
Gestione delle vulnerabilità del ciclo di vita: I produttori sono tenuti a monitorare, identificare e affrontare le vulnerabilità, fornendo aggiornamenti di sicurezza regolari per un periodo minimo specificato (o la vita utile prevista del prodotto).
Trasparenza e conformità: Documentazione e informazioni chiare devono essere fornite agli utenti finali in merito alle funzionalità di sicurezza del prodotto e alla durata del supporto.
Obbligo di segnalazione: Lo sfruttamento attivo delle vulnerabilità o gravi incidenti di sicurezza devono essere segnalati alle autorità nazionali e all'ENISA entro scadenze rigorose.

NILAB GmbH si impegna a garantire la sicurezza dei prodotti e del software che sviluppiamo, compresi i nostri azionamenti per motori lineari (famiglie NLi e GDi) e il software di configurazione NILAB Starter. Apprezziamo il lavoro dei ricercatori di sicurezza e dei clienti che ci aiutano a identificare e affrontare potenziali vulnerabilità e ci impegniamo a lavorare con loro in modo coordinato e costruttivo.

Ambito

Questa politica copre le vulnerabilità che riguardano:
• Motori lineari NILAB con azionamento integrato (famiglie NLi, GDi) e il loro firmware
• NILAB Starter (software di configurazione Windows)
Se non siete certi che un problema rientri in questo ambito, segnalatelo comunque — preferiamo esaminare una segnalazione che risulta fuori ambito piuttosto che perdere un problema reale.

Avviso importante

La disponibilità di questo canale di segnalazione delle vulnerabilità è intesa a supportare una divulgazione responsabile e coordinata delle vulnerabilità. La disponibilità di questo canale di segnalazione non implica certificazione, garanzie di sicurezza o dichiarazioni di conformità relative a qualsiasi prodotto, software, firmware o servizio specifico fornito da **NILAB GmbH**. NILAB valuta e migliora continuamente le caratteristiche di cybersecurity dei suoi prodotti e servizi nell'ambito dei suoi processi di sicurezza del prodotto e gestione delle vulnerabilità. Tutti i problemi segnalati saranno valutati e gestiti secondo i processi di cybersecurity e le procedure di gestione delle vulnerabilità di NILAB.

Come segnalare una vulnerabilità

Segnalate potenziali vulnerabilità di sicurezza utilizzando il nostro modulo di segnalazione online:
https://www.ni-lab.online/SRF/report-vulnerability.php

Quando inviate una segnalazione, includete quante più informazioni possibili tra le seguenti:
• Il prodotto, il modello e la versione firmware/software interessati
• Una descrizione della vulnerabilità e del suo potenziale impatto
• Passaggi per riprodurre il problema o un proof of concept, se disponibile
• Se ritenete che la vulnerabilità sia attivamente sfruttata
• I vostri dati di contatto, se desiderate essere tenuti informati sui progressi (le segnalazioni possono anche essere inviate senza dati di contatto)

Cosa aspettarsi da noi

• Conferma: miriamo a confermare la ricezione della vostra segnalazione entro 3 giorni lavorativi dalla presentazione.
• Triage e indagine: il nostro team valuterà la segnalazione, ne determinerà la validità e la gravità e vi terrà informati sui progressi dove vengono forniti i dati di contatto.
• Divulgazione coordinata: vi chiediamo di non divulgare pubblicamente i dettagli di una vulnerabilità segnalata finché non abbiamo avuto l'opportunità di indagare e, ove applicabile, fornire una correzione. Lavoreremo con voi per concordare una tempistica di divulgazione ragionevole.
• Remediation: una volta confermata una vulnerabilità, la affronteremo tramite un aggiornamento di sicurezza o altre misure di mitigazione appropriate e forniremo ai clienti interessati informazioni e

indicazioni pertinenti.
• Divulgazione pubblica: una volta disponibile una correzione, pubblicheremo informazioni sulla vulnerabilità risolta, compresa una descrizione del problema e dei prodotti interessati, in linea con i nostri obblighi ai sensi delle normative applicabili
(compreso il Cyber Resilience Act dell'UE:
https://digital-strategy.ec.europa.eu/en/policies/cra-summary).

Riservatezza

NILAB GmbH tratterà le segnalazioni di vulnerabilità e le informazioni tecniche associate come riservate e userà tali informazioni esclusivamente allo scopo di indagare, validare, mitigare e correggere i problemi di sicurezza segnalati.

Linee guida per test responsabili

Quando si ricercano potenziali vulnerabilità, vi chiediamo di:
• Evitare azioni che potrebbero danneggiare l'affidabilità o l'integrità dei nostri sistemi, prodotti o dati, o di quelli dei nostri clienti (ad esempio, evitare test su sistemi di produzione che controllano apparecchiature fisiche senza previo coordinamento con noi)
• Non accedere, modificare o cancellare dati che non vi appartengono
• Darci una ragionevole opportunità di indagare e affrontare un problema prima di qualsiasi divulgazione pubblica
• Agire in buona fede e rispettare le leggi applicabili
Non intraprenderemo azioni legali contro ricercatori che agiscono in buona fede e in conformità con questa politica.

Contatto

Per domande su questa politica, o se il modulo di segnalazione non è disponibile, potete contattarci all'indirizzo: **katharina. pirker@nilab. at**

Questa politica fa parte del framework di governance della cybersecurity di NILAB GmbH e supporta i nostri preparativi e obblighi in corso ai sensi del Cyber Resilience Act dell'UE (Regolamento (UE) 2024/2847).

Informazioni di contatto per la sicurezza

NILAB può inoltre pubblicare informazioni di contatto per la sicurezza tramite un file security.txt in conformità con RFC 9116.