Sicherheits- und Offenlegungsrichtlinie für Schwachstellen

Der **Cyber Resilience Act (CRA)** ist eine wegweisende Verordnung der Europäischen Union, die verbindliche Cybersicherheitsanforderungen für Hardware- und Softwareprodukte mit digitalen Elementen festlegt, die auf dem EU-Markt platziert werden. Durch die Behandlung von Schwachstellen im gesamten Produktlebenszyklus zielt der CRA darauf ab, Verbraucher und Unternehmen vor Cyberbedrohungen zu schützen und sicherzustellen, dass “Security by Design” zum Standard für verbundene Geräte wird.

Wichtige Säulen des CRA:

Punkt
Security by Design & Default: Produkte müssen mit optimalen Sicherheitskonfigurationen entwickelt und ausgeliefert werden, um die Angriffsfläche vom ersten Tag an zu minimieren.
Vulnerability-Management über den Lebenszyklus: Hersteller sind verpflichtet, Schwachstellen zu überwachen, zu identifizieren und zu beheben, und regelmäßige Sicherheitsupdates für einen festgelegten Mindestzeitraum (oder die erwartete Lebensdauer des Produkts) bereitzustellen.
Transparenz & Compliance: Klare Dokumentation und Informationen müssen Endbenutzern über die Sicherheitsfunktionen und die Unterstützungsdauer des Produkts bereitgestellt werden.
Meldepflicht: Aktive Ausnutzung von Schwachstellen oder schwerwiegende Sicherheitsvorfälle müssen innerhalb strenger Fristen an nationale Behörden und die ENISA gemeldet werden.

NILAB GmbH ist bestrebt, die Sicherheit der von uns entwickelten Produkte und Software zu gewährleisten, einschließlich unserer Linearmotor-Antriebe (NLi- und GDi-Familien) und der Konfigurationssoftware NILAB Starter. Wir schätzen die Arbeit von Sicherheitsforschern und Kunden, die uns helfen, potenzielle Schwachstellen zu identifizieren und zu beheben, und wir verpflichten uns, in koordinierter und konstruktiver Weise mit ihnen zusammenzuarbeiten.

Geltungsbereich

Diese Richtlinie deckt Schwachstellen ab, die betreffen:
• NILAB Linearmotoren mit integriertem Antrieb (NLi-, GDi-Familien) und ihre Firmware
• NILAB Starter (Windows-Konfigurationssoftware)
Wenn Sie unsicher sind, ob ein Problem in diesen Geltungsbereich fällt, melden Sie es trotzdem — wir prüfen lieber einen Bericht, der sich als außerhalb des Geltungsbereichs herausstellt, als einen realen Fall zu verpassen.

Wichtiger Hinweis

Die Verfügbarkeit dieses Kanals zur Meldung von Schwachstellen soll verantwortungsvolle und koordinierte Offenlegung von Schwachstellen unterstützen. Die Verfügbarkeit dieses Meldekanals bedeutet keine Zertifizierung, Sicherheitsgarantie oder Compliance-Zusage für ein bestimmtes Produkt, Software, Firmware oder Dienstleistung von **NILAB GmbH**. NILAB bewertet und verbessert kontinuierlich die Cybersicherheitsfunktionen seiner Produkte und Dienstleistungen im Rahmen seiner Prozesse für Produktsicherheit und Schwachstellenmanagement. Alle gemeldeten Probleme werden nach den Cybersicherheitsprozessen und Verfahren zum Schwachstellenmanagement von NILAB bewertet und behandelt.

So melden Sie eine Schwachstelle

Bitte melden Sie potenzielle Sicherheitslücken über unser Online-Meldeformular:
https://www.ni-lab.online/SRF/report-vulnerability.php

Geben Sie bei der Einreichung eines Berichts bitte möglichst viele der folgenden Informationen an:
• Das betroffene Produkt, Modell und die Firmware-/Softwareversion
• Eine Beschreibung der Schwachstelle und ihrer potenziellen Auswirkungen
• Schritte zur Reproduktion des Problems oder ein Proof of Concept, falls verfügbar
• Ob Sie glauben, dass die Schwachstelle aktiv ausgenutzt wird
• Ihre Kontaktdaten, wenn Sie über den Fortschritt informiert werden möchten (Berichte können auch ohne Kontaktdaten eingereicht werden)

Was Sie von uns erwarten können

• Bestätigung: Wir bestätigen den Eingang Ihres Berichts innerhalb von 3 Werktagen nach Einreichung.
• Triage und Untersuchung: Unser Team bewertet den Bericht, bestimmt seine Gültigkeit und Schwere und hält Sie über den Fortschritt auf dem Laufenden, wenn Kontaktdaten angegeben sind.
• Koordinierte Offenlegung: Wir bitten Sie, Details einer gemeldeten Schwachstelle nicht öffentlich zu machen, bis wir Gelegenheit hatten, sie zu untersuchen und, falls zutreffend, einen Fix bereitzustellen. Wir werden mit Ihnen einen angemessenen Zeitplan für die Offenlegung vereinbaren.
• Behebung: Sobald eine Schwachstelle bestätigt ist, werden wir sie durch ein Sicherheitsupdate oder

andere geeignete Maßnahmen beheben und betroffene Kunden mit relevanten Informationen und Anleitungen versorgen.
• Öffentliche Offenlegung: Sobald ein Fix verfügbar ist, veröffentlichen wir Informationen über die behobene Schwachstelle, einschließlich einer Beschreibung des Problems und der betroffenen Produkte, im Einklang mit unseren Verpflichtungen nach geltenden Vorschriften (einschließlich des EU Cyber Resilience Act: https://digital-strategy.ec.europa.eu/en/policies/cra-summary).

Vertraulichkeit

NILAB GmbH behandelt Schwachstellenberichte und alle damit verbundenen technischen Informationen vertraulich und verwendet solche Informationen ausschließlich zum Zweck der Untersuchung, Validierung, Abschwächung und Behebung gemeldeter Sicherheitsprobleme.

Richtlinien für verantwortungsvolles Testen

Bei der Erforschung potenzieller Schwachstellen bitten wir Sie:
• Handlungen zu vermeiden, die die Zuverlässigkeit oder Integrität unserer Systeme, Produkte oder Daten oder die unserer Kunden beeinträchtigen könnten (z. B. vermeiden Sie Tests an Produktionssystemen, die physische Ausrüstung steuern, ohne vorherige Koordination mit uns)
• Nicht auf Daten zuzugreifen, sie zu ändern oder zu löschen, die Ihnen nicht gehören
• Uns eine angemessene Gelegenheit zu geben, ein Problem vor einer öffentlichen Offenlegung zu untersuchen und zu beheben
• In gutem Glauben zu handeln und geltende Gesetze einzuhalten
Wir werden keine rechtlichen Schritte gegen Forscher einleiten, die in gutem Glauben und gemäß dieser Richtlinie handeln.

Kontakt

Bei Fragen zu dieser Richtlinie oder wenn das Meldeformular nicht verfügbar ist, erreichen Sie uns unter: **katharina. pirker@nilab. at**

Diese Richtlinie ist Teil des Cybersicherheits-Governance-Rahmens der NILAB GmbH und unterstützt unsere laufenden Vorbereitungen und Verpflichtungen im Rahmen des EU Cyber Resilience Act (Verordnung (EU) 2024/2847).

Kontaktinformationen zur Sicherheit

NILAB kann zusätzlich Sicherheitskontaktinformationen über eine security.txt-Datei gemäß RFC 9116 veröffentlichen.