VARIOLYTICS

Making the invisible visible.

Coordinated Vulnerability Disclosure (CVD) Policy

Richtlinie zur koordinierten Meldung und Offenlegung von Schwachstellen

Unternehmen	Variolytics GmbH
Version	1.0
Stand	August 2026
Status	Freigegeben

1. Zweck dieser Richtlinie

Die Sicherheit unserer Produkte und Systeme hat für die Variolytics GmbH einen hohen Stellenwert. Trotz sorgfältiger Entwicklung, Prüfung und laufender Sicherheitsmaßnahmen können Schwachstellen nicht vollständig ausgeschlossen werden.

Wir begrüßen daher Hinweise von Kunden, Sicherheitsforschenden und anderen Dritten auf mögliche Sicherheitslücken in unseren Produkten. Diese Coordinated Vulnerability Disclosure Policy beschreibt, wie mögliche Schwachstellen an uns gemeldet werden können und wie wir mit entsprechenden Meldungen umgehen.

Unser Ziel ist es, Sicherheitslücken verantwortungsvoll, vertraulich und koordiniert zu untersuchen und zu beheben und Risiken für Nutzer, Kunden und Systeme so weit wie möglich zu reduzieren.

2. Geltungsbereich

Diese Richtlinie gilt für von der Variolytics GmbH bereitgestellte Produkte mit digitalen Elementen und die damit verbundenen Software-, Firmware- und produktbezogenen digitalen Komponenten.

Im Geltungsbereich

- EmiCo lite (vernetztes Messgerät)
- EmiCo Insight (Datenverarbeitungsplattform, Cloud, lokales Gateway oder Kunden-VM)
- Firmware und Embedded Software der genannten Produkte
- zugehörige Softwarekomponenten
- zugehörige Cloud-Dienste, soweit sie Teil der Produktfunktion sind
- zugehörige Webanwendungen und APIs
- von Variolytics bereitgestellte produktbezogene Schnittstellen und Update-Mechanismen
- Drittanbieter- und Open-Source-Komponenten, soweit sie Bestandteil unserer Produkte sind.

Nicht im Geltungsbereich

Sofern nicht ausdrücklich anders vereinbart, fallen insbesondere folgende Systeme oder Aktivitäten nicht unter diese Richtlinie:

- Systeme oder Dienste von Drittanbietern, die nicht von Variolytics betrieben oder kontrolliert werden
- Social-Engineering-Angriffe gegen Mitarbeitende oder Vertragspartner
- physische Angriffe auf Gebäude, Mitarbeitende, Geräte oder Infrastruktur
- Denial-of-Service- oder Distributed-Denial-of-Service-Tests
- Spam, automatisierte Massensendungen oder unnötig hohe automatisierte Abfrageraten
- Tests, die zu einer vermeidbaren Beeinträchtigung der Verfügbarkeit, Integrität oder Funktionsfähigkeit unserer Produkte, Systeme oder Dienstleistungen führen können.

Wenn Sie unsicher sind, ob ein Produkt, System oder eine Testmethode in den Geltungsbereich fällt, kontaktieren Sie uns bitte vor weiteren Tests.

3. Meldung einer Schwachstelle

Wenn Sie eine mögliche Schwachstelle entdecken, senden Sie Ihre Meldung bitte über folgenden Kontaktweg:

Security-E-Mail	security@variolytics.com
Empfohlener Betreff	Security Vulnerability Report – [Produktname]

Um eine schnelle Analyse zu ermöglichen, sollte Ihre Meldung nach Möglichkeit folgende Informationen enthalten:

- betroffenes Produkt bzw. betroffene Komponente
- Modell-, Firmware- oder Softwareversion
- Beschreibung der Schwachstelle und der beobachteten Auswirkungen
- Schritte zur Reproduktion
- gegebenenfalls Proof-of-Concept, Logs, Screenshots oder sonstige technische Nachweise
- verwendete Tools und Testmethoden, soweit für die Reproduktion relevant
- Zeitpunkt der Entdeckung

- Informationen darüber, ob die Schwachstelle bereits Dritten bekannt ist
- gegebenenfalls geplante Veröffentlichung
- Kontaktdaten für Rückfragen.

Bitte übermitteln Sie keine personenbezogenen, vertraulichen oder anderweitig geschützten Informationen, die für die Analyse der Schwachstelle nicht erforderlich sind.

4. Umgang mit Ihrer Meldung

Nach Eingang einer Meldung prüfen wir die bereitgestellten Informationen und bewerten die mögliche Schwachstelle. Unser Prozess umfasst grundsätzlich folgende Schritte:

1. Eingangsbestätigung – Wir bestätigen den Eingang Ihrer Meldung nach Möglichkeit innerhalb von
   3 Werktagen.
2. Erste Bewertung – Wir prüfen die Meldung auf Nachvollziehbarkeit, betroffene Produkte und mögliche Sicherheitsauswirkungen.
3. Technische Analyse – Soweit erforderlich, untersuchen und reproduzieren wir die gemeldete Schwachstelle.
4. Risikobewertung und Priorisierung – Bestätigte Schwachstellen werden anhand ihres Risikos und ihrer möglichen Auswirkungen priorisiert.
5. Behebung oder Risikominderung – Wir entwickeln geeignete Korrektur- oder Risikominderungsmaßnahmen.
6. Bereitstellung eines Sicherheitsupdates – Soweit erforderlich und technisch möglich, stellen wir ein Sicherheitsupdate oder andere geeignete Maßnahmen bereit.
7. Koordinierte Offenlegung – Die Veröffentlichung von Informationen über die Schwachstelle wird mit der meldenden Person soweit möglich abgestimmt.

Wir bemühen uns, meldende Personen über wesentliche Fortschritte bei der Bearbeitung zu informieren. Die konkrete Bearbeitungsdauer hängt insbesondere von der Komplexität, dem Risiko, den betroffenen Komponenten sowie gegebenenfalls erforderlichen Abstimmungen mit Drittanbietern ab.

5. Koordinierte Offenlegung

Bitte veröffentlichen oder teilen Sie detaillierte Informationen über eine noch nicht behobene Schwachstelle nicht ohne vorherige Abstimmung mit uns.

Wir bitten Sie insbesondere darum, Variolytics ausreichend Zeit für die Analyse der Schwachstelle, die Entwicklung und Prüfung einer geeigneten Behebung, die Bereitstellung von Sicherheitsupdates und die Information betroffener Nutzer einzuräumen.

Variolytics wird seinerseits darauf hinwirken, bestätigte Schwachstellen ohne unangemessene Verzögerung zu behandeln. Nach Bereitstellung einer geeigneten Korrekturmaßnahme können Variolytics und die meldende Person einen geeigneten Zeitpunkt und Umfang einer Veröffentlichung abstimmen.

In begründeten Fällen kann eine Veröffentlichung verschoben werden, wenn eine frühzeitige Offenlegung zu einem erhöhten Sicherheitsrisiko für Nutzer oder Systeme führen würde.

6. Verantwortungsvolle Sicherheitsforschung

Wir bitten Sicherheitsforschende, bei Untersuchungen nach Treu und Glauben, verhältnismäßig und verantwortungsvoll vorzugehen. Bitte:

- führen Sie nur Tests durch, die zur Identifikation und Verifizierung einer Schwachstelle erforderlich sind;
- vermeiden Sie Beeinträchtigungen der Verfügbarkeit oder Funktionsfähigkeit unserer Produkte und Systeme;
- greifen Sie nicht auf Daten anderer Nutzer zu und verändern oder löschen Sie keine Daten;
- kopieren Sie keine Daten, sofern dies nicht zwingend erforderlich ist, um die Schwachstelle nachzuweisen;
- beenden Sie Tests, sobald Sie unbeabsichtigt auf personenbezogene, vertrauliche oder anderweitig geschützte Daten zugreifen;
- führen Sie keine Social-Engineering-Angriffe durch;

- installieren Sie keine Schadsoftware oder dauerhaften Zugänge;
- nutzen Sie eine entdeckte Schwachstelle nicht zum eigenen oder fremden Vorteil aus;
- geben Sie Informationen über eine Schwachstelle nicht an Dritte weiter, bevor eine koordinierte Offenlegung erfolgt ist.

Sollten Sie während Ihrer Untersuchung unbeabsichtigt auf sensible Daten zugreifen, beenden Sie den Zugriff und informieren Sie uns unverzüglich.

7. Umgang mit Sicherheitsforschenden

Wenn Sie Sicherheitsforschung in gutem Glauben, im Rahmen dieser Richtlinie und ohne schädliche Absicht durchführen, beabsichtigt Variolytics – soweit rechtlich zulässig – nicht, allein aufgrund dieser Sicherheitsforschung rechtliche Schritte gegen Sie einzuleiten.

Dies gilt insbesondere nur, sofern:

- die Untersuchung verhältnismäßig erfolgt;
- keine unnötigen Schäden oder Betriebsbeeinträchtigungen verursacht werden;
- keine Daten missbräuchlich verwendet werden;
- keine Erpressungs- oder Zahlungsforderungen mit der Nichtveröffentlichung einer Schwachstelle verbunden werden;
- die Schwachstelle entsprechend dieser Policy koordiniert gemeldet wird.

> Diese Erklärung stellt keine allgemeine Genehmigung dar, gegen geltendes Recht, vertragliche Verpflichtungen oder Rechte Dritter zu verstoßen.

8. Sicherheitsupdates und Informationen

Bestätigte Schwachstellen werden entsprechend ihres Risikos behandelt. Soweit erforderlich, stellen wir Sicherheitsupdates oder andere geeignete Maßnahmen zur Behebung oder Reduzierung des Risikos zur Verfügung.

Veröffentlichte Sicherheitsinformationen können insbesondere folgende Angaben enthalten:

- betroffenes Produkt und betroffene Versionen
- Beschreibung und Sicherheitsauswirkungen der Schwachstelle
- Schweregrad bzw. Priorisierung
- behobene Version und verfügbare Sicherheitsupdates
- erforderliche Maßnahmen oder Empfehlungen für Nutzer.

Sicherheitsinformationen werden veröffentlicht unter: https://variolytics.com/security

9. Schwachstellen in Komponenten von Drittanbietern

Unsere Produkte können Software-, Hardware- oder Open-Source-Komponenten von Drittanbietern enthalten. Wenn eine gemeldete Schwachstelle eine solche Komponente betrifft, können wir Informationen über die Schwachstelle an den jeweiligen Hersteller, Anbieter oder Maintainer weitergeben, soweit dies für die Analyse und Behebung erforderlich und rechtlich zulässig ist.

Dabei achten wir auf eine koordinierte und verantwortungsvolle Weitergabe der Informationen.

10. Gesetzliche Meldepflichten

Bestimmte Schwachstellen oder Sicherheitsvorfälle können gesetzlichen Meldepflichten unterliegen. Variolytics behält sich daher vor, Informationen über gemeldete Schwachstellen im gesetzlich erforderlichen Umfang an zuständige Behörden, Computer Security Incident Response Teams (CSIRTs) oder andere nach geltendem Recht vorgesehene Stellen weiterzugeben.

Dies gilt insbesondere für Meldepflichten nach der Verordnung (EU) 2024/2847 (Cyber Resilience Act).

11. Vergütung

Variolytics betreibt derzeit kein Bug-Bounty-Programm. Die Meldung einer Schwachstelle begründet daher grundsätzlich keinen Anspruch auf eine finanzielle Vergütung.

12. Kontakt

Unternehmen	Variolytics GmbH
Postanschrift	Ruppmannstraße 28, 70565 Stuttgart
Security-Kontakt	security@variolytics.com
Website	https://www.variolytics.com
CVD Policy	https://variolytics.com/security
Security Advisories	https://variolytics.com/security

Diese Policy kann bei Bedarf aktualisiert werden. Maßgeblich ist die jeweils auf unserer Website veröffentlichte Fassung.