CVD (Coordinated Vulnerability Disclosure)-Policy

1. Einleitung und Geltungsbereich (Scope)

Bei **VEGA** hat die Sicherheit unserer Produkte mit digitalen Elementen hohe Priorität. Diese Policy beschreibt, wie Sie eine mögliche Schwachstelle in unseren Produkten an uns melden können und wie wir mit Ihrer Meldung umgehen. Wir begrüßen Meldungen von Sicherheitsforschenden, Kundinnen und Kunden, Partnern und der Öffentlichkeit.

Geltungsbereich: Diese Policy gilt für folgende Produkte und Dienste:

- Alle VEGA-Geräte, erkennbar an dem Gerätenamen „VEGA…“
- PROTRAC-Serie (MINITRAC, PIONTRAC, WEIGHTRAC, FIBERTRAC, SOLITRAC)
- PLICSCOM
- PLICSMOBILE
- VEGA Tools App
- VEGA Inventory System
- VEGA DTM Collection
- VEGA DataViewer

Nicht im Geltungsbereich sind: Produkte und Dienste der VEGA, mit ausgesprochener End-of-Life.

2. Kontaktmöglichkeiten zur Meldung

Sie erreichen unser Sicherheitsteam über folgende Kanäle:

- E-Mail: psirt@vega.com
- Telefon: +49 7836 50-0

3. Inhalt einer Schwachstellenmeldung

Damit wir Ihre Meldung schnell bearbeiten können, geben Sie bitte folgende Informationen an:

- **Bezeichnung des betroffenen Produkts***
- Version (z. B. HW-Version, SW-Version, Tool-Version)
- Umgebung (z. B. Kombination mit anderen VEGA Geräten, Betriebssystem)
- **Beschreibung der Schwachstelle und der möglichen Auswirkung***
- Schritte zur Reproduktion

*Pflichtinformationen

4. Ablauf und laufende Kommunikation

Nach Eingang Ihrer Meldung gehen wir wie folgt vor:

1. Eingangsbestätigung innerhalb von 2 Werktagen, mit Vergabe einer eindeutigen Tracking-Nummer.

2. Prüfung und Verifikation der gemeldeten Schwachstelle.
3. Statusmeldungen in Abständen von 20 Tagen.
4. Behebung und Veröffentlichung gemäß Abschnitt 6–7.

5. Sichere und anonyme Kommunikation

Schwachstelleninformationen sind sensibel. Sollten Sie Ihre Nachricht verschlüsseln wollen, ist dies über CERT@VDE möglich. Wir akzeptieren Meldungen auch dann, wenn kein sicherer Kanal genutzt werden kann.

Bitte hinterlegen Sie grundsätzlich gültige Kontaktdaten (z. B. E-Mail-Adresse), damit wir Sie im Falle von Rückfragen kontaktieren können. Wir versprechen jeden Schwachstellenbericht innerhalb des gesetzlichen Rahmens vertraulich zu behandeln. Personenbezogene Daten werden nicht ohne Ihre ausdrückliche Zustimmung an Dritte weitergegeben.

Anonyme Meldung: Sie können auch anonym melden.

6. Offenlegungsstrategie und Embargo

Wir folgen dem Prinzip der koordinierten Offenlegung: Details werden erst veröffentlicht, wenn eine Behebung verfügbar ist. Wir vereinbaren einen angemessenen Embargo-Zeitraum (Richtwert 90 Tage), der je nach Komplexität und Kritikalität im Einzelfall angepasst werden kann.

7. Veröffentlichung

Nach Behebung veröffentlichen wir ein Security Advisory. Unsere veröffentlichten Advisories finden Sie im Advisory-Portal des CERT@VDE: https://certvde.com/de/advisories/vendor/vega/

Wir betreiben **kein** Bug-Bounty-Programm.

8. Rechtlicher Rahmen

Wir erwarten von Ihnen, dass die gefundene Schwachstelle nicht missbräuchlich von Ihnen ausgenutzt wurde und dass Sie keine Angriffe gegen bzw. keine Manipulation, Kompromittierung oder Veränderung von VEGA-Produkten und VEGA-Tools durchgeführt haben.

Wir versprechen, keine strafrechtlichen Schritte gegen Sie einzuleiten, solange Ihrerseits die Richtlinie und Grundsätze eingehalten wurden. Dies gilt nicht, wenn erkennbare kriminelle Absichten verfolgt wurden oder werden.