

RICHTLINIE ZUR KOORDINIERTEN OFFENLEGUNG VON SICHERHEITSLÜCKEN (CVD)

DOMEL d.o.o.

Zweck: Domel unterstützt die verantwortungsvolle Meldung und koordinierte Behandlung von Sicherheitslücken, um Anwender, Produkte und damit verbundene Dienstleistungen zu schützen.

Geltungsbereich: Diese Richtlinie gilt für Produkte mit digitalen Elementen, Firmware, Software, Kommunikationsschnittstellen sowie zugehörige digitale Dienste.

Meldung von Sicherheitslücken: Sicherheitslücken können per E-Mail an psirt@domel.com gemeldet werden. Anonyme Meldungen werden akzeptiert. Meldungen können auf Slowenisch oder Englisch eingereicht werden.

Erforderliche Angaben: Eine Meldung sollte folgende Informationen enthalten:

- Betroffenes Produkt und Modell
- Hardware-, Firmware- und Softwareversion (HW/FW/SW)
- Beschreibung der Sicherheitslücke und ihrer möglichen Auswirkungen
- Schritte zur Reproduktion der Sicherheitslücke
- Machbarkeitsnachweis (Proof of Concept), sofern verfügbar
- Angaben zum aktuellen Veröffentlichungsstatus der Sicherheitslücke
- Kontaktdaten des Meldenden (optional)

Bearbeitungsprozess: Domel bestätigt den Eingang einer Meldung innerhalb von **3 Arbeitstagen** und führt innerhalb von **10 Arbeitstagen** eine erste Bewertung durch. Die Behebung bestätigter Sicherheitslücken erfolgt schnellstmöglich.

Koordinierte Offenlegung: Wir bitten darum, Details zu Sicherheitslücken nicht öffentlich bekannt zu geben, bevor eine Sicherheitskorrektur bereitgestellt wurde oder ein gemeinsam vereinbarter Veröffentlichungstermin erreicht ist.

Grundsatz des Handelns nach Treu und Glauben: Domel wird keine rechtlichen Schritte gegen Personen einleiten, die in gutem Glauben und im Einklang mit dieser Richtlinie handeln.

Sicherheitshinweise:

<https://www.domel.com/de/uber-uns/das-product-security-incident-response-team>

PSIRT-Kontakt:

psirt@domel.com