RICHTLINIE

Richtlinie zur koordinierten Offenlegung von Schwachstellen

Traeger GmbH Industry Components

DOKUMENTSTEUERUNG

MERKMAL	WERT
Version	1.0
Stand	10. November 2026
Status	Freigegeben
Klassifizierung	Öffentlich

Traeger GmbH Industry Components · Söllnerstraße 9 · 92637 Weiden i.d. OPf. · traeger.de
Amtsgericht Weiden i.d. OPf., HRB 1882 · Geschäftsführer: B. Sc. Dominik Scharnagl

Inhalt

Kapitel 1 · Zweck dieser Richtlinie **3**
Geltungsbereich 3
Kapitel 2 · Meldeweg **4**
Inhalt einer Schwachstellenmeldung 4
Bearbeitungsverfahren 4
Reaktionszeiten 5
Kapitel 3 · Koordinierte Offenlegung **5**
Safe Harbor — Rechtsverzicht 6
Reverse Engineering und Dekompilierung 6
Koordination mit Dritten 7
Kapitel 4 · Meldepflichten gemäß Cyber Resilience Act **7**
Kein Bug-Bounty-Programm 7
Datenschutz 8
Kapitel 5 · Eskalation **8**
Hinweise zu unseren Produkten 8
Ausschlüsse 8
Geltung und Änderungen 9
Kontakt 9

SICHERHEITSMELDUNGEN	MASCHINENLESBAR	STANDARDS & REFERENZEN	ESKALATION
psirt@traeger.de OpenPGP verfügbar Deutsch oder Englisch	`/.well-known/security.txt` gemäß RFC 9116 `/.well-known/pgp-key.asc`	ISO/IEC 29147:2018 BSI-CS_019 FIRST PSIRT Services Framework	BSI als Vermittler vulnerability@bsi.bund.de

Kapitel 1 · Zweck dieser Richtlinie

Die Traeger GmbH Industry Components (nachfolgend „Traeger“) ist Hersteller industrieller Softwarelösungen. Die Sicherheit unserer Produkte hat für uns höchste Priorität.

Diese Richtlinie beschreibt, wie Sicherheitsforscher, Kunden und Dritte eine mögliche Schwachstelle in unseren Produkten melden können, wie wir mit solchen Meldungen umgehen, und unter welchen Bedingungen eine koordinierte Veröffentlichung erfolgt.

Wir orientieren uns an den Empfehlungen der **ISO/IEC 29147:2018** (Vulnerability Disclosure), des **BSI** (BSI-CS_019) sowie am **FIRST PSIRT Services Framework**. Diese Richtlinie ist Bestandteil unserer CRA-Compliance gemäß der EU-Verordnung über horizontale Cybersicherheitsanforderungen (Cyber Resilience Act).

Geltungsbereich

Eingeschlossen

Alle von Traeger aktiv vertriebenen Softwareprodukte in der jeweils aktuellen sowie den innerhalb des Unterstützungszeitraums liegenden Versionen.

Ausgeschlossen

- Die Webseite traeger.de und alle damit verbundenen Webdienste (z.B. `docs.traeger.de`, `share.traeger.de`). Für Schwachstellen in unserer Webinfrastruktur wenden Sie sich bitte an info@traeger.de.
- Produkte, die ihr **End-of-Life** im Sinne unserer CRA-Compliance erreicht haben und nicht mehr aktiv vertrieben werden.
- **Drittanbieter-Software**, die in unseren Produkten enthalten ist (z.B. Open-Source-Bibliotheken). Schwachstellen in diesen Komponenten nehmen wir dennoch entgegen und leiten sie gegebenenfalls an den jeweiligen Upstream-Maintainer weiter.

Kapitel 2 · Meldeweg

Sicherheitsmeldungen richten Sie bitte ausschließlich an unseren PSIRT-Kanal. Dieser ist von unserem allgemeinen Kundensupport getrennt, damit Sicherheitsmeldungen sofort den richtigen Personenkreis erreichen.

E-Mail	psirt@traeger.de
Verschlüsselung	OpenPGP — öffentlicher Schlüssel verfügbar unter `/.well-known/pgp-key.asc`
Maschinenlesbar	`/.well-known/security.txt` (gemäß RFC 9116)
Sprache	Deutsch oder Englisch

Bitte verwenden Sie für Sicherheitsmeldungen nicht unsere allgemeine info@- oder support@-Adresse. Meldungen an diese Adressen können Verzögerungen unterliegen.

Inhalt einer Schwachstellenmeldung

Eine aussagekräftige Meldung hilft uns, die Schwachstelle schnell zu bewerten und zu beheben. Wir bitten Sie, nach Möglichkeit folgende Informationen bereitzustellen:

- **Betroffenes Produkt und Version** (z.B. Opc.UaFx.Advanced 2.51.4.0)
- **Beschreibung der Schwachstelle** und ihrer möglichen Auswirkung
- **Schritte zur Reproduktion** oder ein Proof-of-Concept
- **Ihre eigene Einschätzung des Schweregrads** (z.B. CVSS-Score)
- **Ihre Kontaktdaten** für Rückfragen (E-Mail genügt)
- Ob Sie bei Veröffentlichung einer Security Advisory **namentlich als Melder genannt** werden möchten oder anonym bleiben wollen

Meldungen, die nicht alle Informationen enthalten, werden selbstverständlich dennoch bearbeitet.

Bearbeitungsverfahren

Nach Eingang Ihrer Meldung durchläuft diese folgende Schritte:

1. **Eingangsbestätigung** — Wir bestätigen den Eingang Ihrer Meldung innerhalb der unten genannten Erstreaktion-Zielzeiten.
2. **Bewertung** — Wir bewerten die Schwachstelle nach CVSS v3.1 und ordnen ihr einen Schweregrad zu (Critical, High, Medium, Low).
3. **Behebung** — Wir entwickeln einen Fix oder Workaround und stellen diesen innerhalb der unten genannten Zielzeiten bereit.

4. **Kommunikation** — Während der Bearbeitung halten wir Sie über den Stand auf dem Laufenden, von der ersten Bewertung über die Entwicklung des Fixes bis zur Veröffentlichung.
5. **Veröffentlichung** — Nach Bereitstellung des Fixes veröffentlichen wir eine Security Advisory (siehe Kapitel 3).

Reaktionszeiten

Die folgenden Zielzeiten gelten ab Eingang der Meldung:

SCHWEREGRAD	ERSTREAKTION	FIX-ZIEL
Critical CVSS 9,0–10,0	Innerhalb 24 Stunden	Hotfix innerhalb 7 Tagen; Workaround sofort, sobald verfügbar
High CVSS 7,0–8,9	Innerhalb 48 Stunden	Hotfix innerhalb 14 Tagen
Medium CVSS 4,0–6,9	Innerhalb 5 Werktagen	Nächstes reguläres Release
Low CVSS 0,1–3,9	Innerhalb 10 Werktagen	Nächstes reguläres Release

Erstreaktion-Zielzeiten beziehen sich auf unsere Geschäftszeiten (Mo–Fr). Meldungen, die außerhalb dieser Zeiten eingehen, werden am nächsten Geschäftstag bearbeitet. Diese Zielzeiten sind unsere Selbstverpflichtung. Die tatsächliche Bearbeitungsdauer kann von der Komplexität der Schwachstelle und der Verfügbarkeit von Patches in betroffenen Drittabhängigkeiten abhängen.

Kapitel 3 · Koordinierte Offenlegung

Wir praktizieren **Coordinated Vulnerability Disclosure**. Das bedeutet:

- **Embargo-Zeitraum** — Nach Eingang einer Meldung beginnt ein Embargo-Zeitraum von 90 Tagen. Während dieses Zeitraums bitten wir den Melder, keine Informationen über die Schwachstelle öffentlich zu machen.
- **Veröffentlichung durch Traeger** — Wir veröffentlichen eine Security Advisory, sobald ein Fix oder ein Workaround verfügbar ist — idealerweise vor Ablauf des Embargo-Zeitraums.
- **Veröffentlichung durch den Melder** — Nach Ablauf der 90 Tage steht es dem Melder frei, die Schwachstelle zu veröffentlichen — unabhängig davon, ob ein Fix verfügbar ist. Wir bitten in diesem Fall um vorherige Abstimmung, damit wir die Veröffentlichung unserer Advisory koordinieren können.

- **Ausnahme bei aktiver Ausnutzung** — Bei Schwachstellen mit einem Schweregrad Critical (CVSS ≥ 9,0) prüfen wir im Rahmen der Bewertung aktiv, ob Hinweise auf eine Ausnutzung vorliegen. Wir beziehen dabei auch die Einschätzung des Melders ein. Liegen solche Hinweise vor, entfällt das Embargo zugunsten einer sofortigen Benachrichtigung betroffener Kunden und der behördlichen Meldung gemäß Kapitel 4. In diesem Fall informieren wir den Melder vorab.
- **Anerkennung des Melders** — Auf Wunsch nennen wir den Melder namentlich in der veröffentlichten Advisory. Standardmäßig erfolgt die Anerkennung anonym („Mit Dank an einen verantwortungsvollen Melder"). Die Entscheidung liegt beim Melder.

Safe Harbor — Rechtsverzicht

Traeger verzichtet darauf, rechtliche Schritte gegen Personen einzuleiten, die Schwachstellen in unseren Produkten im Rahmen dieser Richtlinie melden, sofern folgende Bedingungen eingehalten werden:

- Die Meldung erfolgt **in gutem Glauben** und mit dem Ziel, die Sicherheit unserer Produkte zu verbessern.
- Der Melder hat **keinen unbefugten Zugriff** auf personenbezogene Daten Dritter vorgenommen, diese kopiert, verändert oder weitergegeben.
- Der Melder hat **keine Verfügbarkeit unserer Systeme** oder der Systeme unserer Kunden beeinträchtigt (z.B. durch Denial-of-Service Tests).
- Der Melder hat die Schwachstelle **nicht öffentlich gemacht**, bevor Traeger die Möglichkeit hatte, einen Fix bereitzustellen oder der Embargo-Zeitraum abgelaufen ist.
- Der Melder hat die Schwachstelle **nicht für Erpressung, Nötigung** oder sonstige rechtswidrige Zwecke verwendet.

Dieser Verzicht erstreckt sich auf Ansprüche aus dem **Strafrecht (§§ 202a–202c StGB)**, dem **Urheberrecht (UrhG)** und dem **Geschäftsgeheimnisgesetz (GeschGehG)**, soweit die oben genannten Bedingungen erfüllt sind.

> Diese Zusicherung gilt nicht für Handlungen, die erkennbar mit krimineller Absicht erfolgen oder die über das zur Identifikation und Dokumentation der Schwachstelle erforderliche Maß hinausgehen.

Reverse Engineering und Dekompilierung

Sicherheitsforschung kann die Analyse von Binärdateien erfordern. Für Analysen, die ausschließlich der Identifikation von Sicherheitsschwachstellen dienen und deren Ergebnisse uns im Rahmen dieser Richtlinie gemeldet werden, erheben wir keine Ansprüche aus **§§ 69c, 69e UrhG** (Dekompilierungsverbot) oder dem **Geschäftsgeheimnisgesetz**.

Voraussetzung ist, dass die Analyse auf das zur Identifikation der Schwachstelle erforderliche Maß beschränkt bleibt und gewonnene Erkenntnisse nicht für andere Zwecke als die Schwachstellenmeldung verwendet werden.

Koordination mit Dritten

Unsere Produkte integrieren Drittanbieter-Komponenten, darunter Open-Source-Bibliotheken und Spezifikationen der OPC Foundation. Wenn eine gemeldete Schwachstelle eine solche Drittkomponente betrifft, koordinieren wir die Offenlegung mit dem jeweiligen Upstream-Maintainer oder der zuständigen Organisation.

In solchen Fällen kann sich der Embargo-Zeitraum verlängern, da die Behebung von der Kooperation Dritter abhängt. Wir informieren den Melder über die Einbindung Dritter und den angepassten Zeitplan.

Kapitel 4 · Meldepflichten gemäß Cyber Resilience Act

Als Hersteller unterliegen wir seit dem **11. September 2026** den Meldepflichten des EU Cyber Resilience Act. Das bedeutet:

Aktiv ausgenutzte Schwachstellen

Wenn uns Hinweise vorliegen, dass eine Schwachstelle aktiv ausgenutzt wird, melden wir diese innerhalb von **24 Stunden** an die ENISA und das zuständige nationale CSIRT (BSI/CERT-Bund). Innerhalb von **72 Stunden** folgt ein detaillierter Bericht.

Schwere Sicherheitsvorfälle

Sicherheitsvorfälle, die die Integrität unserer Produkte betreffen, melden wir ebenfalls an die zuständigen Behörden.

Diese behördlichen Meldepflichten sind unabhängig vom Embargo-Zeitraum gegenüber dem Melder. **Eine behördliche Meldung bedeutet keine öffentliche Offenlegung der Schwachstelle.**

Kein Bug-Bounty-Programm

Traeger betreibt **kein Bug-Bounty-Programm** und zahlt keine finanziellen Anreize für Schwachstellenmeldungen. Wir schätzen die Beiträge von Sicherheitsforschern und bieten auf Wunsch eine namentliche Anerkennung in der veröffentlichten Security Advisory an.

Datenschutz

Personenbezogene Daten, die im Rahmen einer Schwachstellenmeldung erhoben werden (insbesondere Name und E-Mail-Adresse des Melders), verarbeiten wir ausschließlich zum Zweck der Bearbeitung der Meldung und der Kommunikation mit dem Melder. Die Verarbeitung erfolgt auf Grundlage von **Art. 6 Abs. 1 lit. f DSGVO** (berechtigtes Interesse an der Produktsicherheit).

Melderdaten werden nicht an Dritte weitergegeben, es sei denn, dies ist zur Koordination mit Upstream-Maintainern erforderlich und der Melder hat dem zugestimmt. Die Daten werden gelöscht, sobald die Bearbeitung der Meldung und die Veröffentlichung der Advisory abgeschlossen sind, spätestens jedoch **nach 24 Monaten**.

Kapitel 5 · Eskalation

Sollte ein Melder den Eindruck haben, dass seine Meldung nicht angemessen bearbeitet wird, steht es ihm frei, das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** als Vermittler einzuschalten. Das BSI bietet einen Koordinationsdienst für Fälle, in denen die direkte Kommunikation zwischen Melder und Hersteller nicht zum gewünschten Ergebnis führt.

BSI-Kontakt für Schwachstellenmeldungen: vulnerability@bsi.bund.de

Hinweise zu unseren Produkten

Für Sicherheitsforscher, die das Verhalten unserer Produkte analysieren, ist folgender Kontext relevant:

- Unsere Produkte kommunizieren **nicht „nach Hause“**. Es gibt keine Telemetrie, keinen Analytics-Endpunkt und keinen automatischen Update-Check zu Traeger-Servern.
- Sicherheitspatches werden als **Revision-Increment** bereitgestellt (`Major.Minor.Build.Revision`). Eine Änderung im vierten Versionssegment kennzeichnet einen gezielten Fix ohne funktionale Änderungen.
- **SBOM-Daten im SPDX-2.3-Format** sind Bestandteil jedes Produkt-Downloads und können für die Identifikation betroffener Drittkomponenten verwendet werden.

Ausschlüsse

Folgende Aktivitäten fallen **nicht** unter den Schutz dieser Richtlinie und werden von uns nicht als koordinierte Schwachstellenmeldung anerkannt:

- Penetrationstests gegen Produktivsysteme von Traeger-Kunden ohne deren ausdrückliche Zustimmung
- Social Engineering gegen Mitarbeiter von Traeger oder deren Kunden

- Denial-of-Service-Angriffe jeder Art
- Zugriff auf, Kopie von oder Veränderung personenbezogener Daten Dritter
- Erpressung oder Nötigung in Verbindung mit einer Schwachstellenmeldung
- Öffentliche Diskussion oder Veröffentlichung einer Schwachstelle vor Ablauf des Embargo-Zeitraums oder vor Abstimmung mit Traeger

Geltung und Änderungen

Diese Richtlinie tritt mit ihrer Veröffentlichung unter https://www.traeger.de/security/cvd-policy in Kraft.

Traeger behält sich vor, die Richtlinie jederzeit zu aktualisieren. Änderungen werden unter derselben URL veröffentlicht und mit einem aktualisierten Versionsdatum versehen. Die jeweils aktuelle Fassung ist unter `/.well-known/security.txt` referenziert.

Für Meldungen, die vor einer Änderung der Richtlinie eingegangen sind, gilt die zum Zeitpunkt der Meldung gültige Fassung.

Kontakt

Sicherheitsmeldungen	psirt@traeger.de (OpenPGP verfügbar)
Compliance-Anfragen	info@traeger.de
Service-Vertrag	sales@traeger.de
Telefon	+49 961 48 23 0-0
Anschrift	Traeger GmbH Industry Components Söllnerstraße 9 92637 Weiden i.d. OPf.