Richtlinie zur koordinierten Offenlegung von Schwachstellen (CVD Policy)

1. Einleitung

Die PROMESS Gesellschaft für Montage- und Prüfsystem mbH legt höchsten Wert auf die Sicherheit und Zuverlässigkeit ihrer Produkte und digitalen Dienste. Wir begrüßen das Feedback von Sicherheitsforschern, Kunden und der breiten Öffentlichkeit, um unsere IT-Sicherheit kontinuierlich zu verbessern.

Wenn Sie glauben, eine Schwachstelle, ein Datenschutzproblem, offenliegende Daten oder andere Sicherheitsrisiken in unseren Systemen oder Produkten entdeckt zu haben, möchten wir von Ihnen hören. Diese Richtlinie beschreibt die Schritte zur Meldung von Schwachstellen an uns, unsere Erwartungen an Sie sowie das, was Sie von uns erwarten können.

2. Geltungsbereich

Diese Richtlinie gilt für alle von der PROMESS in Verkehr gebrachten Produkte mit digitalen Elementen innerhalb ihres gesetzlichen Support-Zeitraums gemäß dem EU Cyber Resilience Act (CRA).

Außerhalb des Geltungsbereichs

IT-Systeme, physische Geräte, Cloud-Infrastrukturen oder andere Assets, die Eigentum von Dritten (z. B. Zulieferern, Partnern oder Kunden) sind.

Schwachstellen, die in Systemen außerhalb unseres Geltungsbereichs entdeckt oder vermutet werden, sollten direkt dem entsprechenden Hersteller oder der zuständigen Behörde gemeldet werden.

3. Unsere Zusagen

Wenn Sie im Rahmen dieser Richtlinie mit uns zusammenarbeiten, können Sie von uns Folgendes erwarten:

- Wir bestätigen den Erhalt Ihrer Schwachstellenmeldung unverzüglich, in der Regel innerhalb von 48 Stunden (bzw. 2 Werktagen).

- Wir validieren Ihre Meldung und halten Sie im Rahmen des Triage- und Behebungsprozesses über wesentliche Fortschritte auf dem Laufenden.

- Wir arbeiten mit Nachdruck daran, verifizierte Schwachstellen ohne unangemessene Verzögerung und innerhalb unserer betrieblichen Möglichkeiten durch Sicherheitsupdates oder Schutzmaßnahmen zu beheben.

- Wir gewähren Ihnen vollumfänglichen Schutz vor rechtlichen Schritten, sofern Sie sich an die Bedingungen dieser Richtlinie halten.

4. Unsere Erwartungen an Sicherheitsforscher

Zur Gewährleistung einer verantwortungsvollen und koordinierten Offenlegung bitten wir Sie um die Einhaltung folgender Regeln:

- Halten Sie sich an diese Richtlinie, sowie an alle anderen relevanten Vereinbarungen. Falls Widersprüche zwischen dieser Richtlinie und anderen Nutzungsbedingungen der PROMESS bestehen, haben die Bestimmungen dieser Richtlinie Vorrang.

- Melden Sie uns jede von Ihnen entdeckte Schwachstelle unverzüglich nach deren Entdeckung.

- Vermeiden Sie jede Beeinträchtigung der Verfügbarkeit unserer Dienste (z.B. durch DoS/DDoS-Angriffe), die Zerstörung von Daten sowie die Beeinträchtigung der Nutzererfahrung unserer Kunden.

- Kommunizieren Sie technische Details zu Schwachstellen ausschließlich über unsere offiziellen Kanäle und verzichten Sie auf eine vorzeitige Veröffentlichung.

- Geben Sie uns eine angemessene Zeitspanne von mindestens 90 Tagen ab der Erstmeldung, um das Problem zu beheben, bevor Sie Informationen darüber öffentlich machen.

- Führen Sie Tests nur an Systemen durch, die im Geltungsbereich liegen, und respektieren Sie Systeme, die außerhalb des Geltungsbereichs liegen.

Minimierung des Datenzugriffs & Datenschutz:

- Falls eine Schwachstelle einen unbeabsichtigten Zugriff auf Daten ermöglicht: Beschränken Sie den Datenzugriff auf das für den Machbarkeitsnachweis (Proof of Concept) absolut erforderliche Minimum.

- Stellen Sie die Tests sofort ein und senden Sie uns umgehend eine Meldung, wenn Sie während des Tests auf personenbezogene Daten (PII), geschützte Gesundheitsdaten (PHI), Kreditkartendaten oder geschäftlich geschützte Informationen stoßen. Löschen Sie lokal gecachte Kopien solcher Daten unverzüglich.

- Interagieren Sie nur mit Testkonten, die Sie selbst besitzen, oder für die Ihnen eine ausdrückliche Erlaubnis des Kontoinhabers vorliegt.

- Verwenden Sie Schwachstellenmeldungen nicht zur Erpressung, Nötigung oder für unberechtigte finanzielle Forderungen.

5. Offizielle Kanäle & Meldeweg

Bitte senden Sie Schwachstellenmeldungen per E-Mail an:

E-Mail: security@promessmontage.de

Empfohlene Angaben in Ihrer Meldung:

Um uns eine schnelle Validierung und Behebung zu ermöglichen, sollte Ihre Meldung idealerweise folgende Informationen enthalten:

1. Eine detaillierte Beschreibung der Schwachstelle (inkl. betroffener URL, IP-Adresse, Produktname oder Softwareversion).

2. Eine Schritt-für-Schritt-Anleitung oder ein Skript zur Reproduktion des Fehlers (Proof of Concept).

3. Eine Einschätzung der potenziellen Auswirkungen und des Schweregrads (z. B. CVSS-Score, falls bekannt).

6. Safe Harbor

Bei der Durchführung von Schwachstellenanalysen im Rahmen dieser Richtlinie betrachten wir Ihre Aktivitäten als:

- Autorisiert im Hinblick auf alle anwendbaren Gesetze gegen Computerkriminalität. Wir werden keine rechtlichen Schritte gegen Sie einleiten oder unterstützen, wenn Sie versehentlich und in gutem Glauben im Rahmen dieser Richtlinie handeln.

- Autorisiert im Hinblick auf geltende Gesetze zur Umgehung von technischen Schutzmaßnahmen. Wir werden keine Ansprüche wegen der Umgehung technologischer Kontrollmechanismen gegen Sie geltend machen.

- Befreit von den restriktiven Bestimmungen in unseren Allgemeinen Geschäftsbedingungen (AGB) oder Nutzungsbedingungen, die einer Sicherheitsanalyse im Wege stehen würden. Wir setzen diese Beschränkungen für die Dauer und den Zweck der Analyse aus.

- Rechtmäßig, hilfreich für die allgemeine Sicherheit des Internets und in gutem Glauben durchgeführt.

Es wird von Ihnen erwartet, dass Sie alle geltenden Gesetze einhalten. Falls ein Dritter rechtliche Schritte gegen Sie einleitet und Sie diese Richtlinie eingehalten haben, werden wir offiziell bestätigen, dass Ihre Handlungen in Übereinstimmung mit dieser Richtlinie erfolgt sind.

Wichtige Einschränkungen:

- Wenn Sie zu irgendeinem Zeitpunkt unsicher sind, ob Ihre Sicherheitsforschung mit dieser Richtlinie vereinbar ist, kontaktieren Sie uns bitte über unseren offiziellen Kanal, bevor Sie fortfahren.

Bitte beachten Sie, dass der „Sichere Hafen" nur für rechtliche Ansprüche gilt, die der direkten Kontrolle der PROMESS unterliegen, und diese Richtlinie unabhängige Dritte nicht binden kann.