Coordinated Vulnerability Disclosure Policy

Die Software-Schmiede Vogler & Hauke GmbH nimmt Hinweise auf potenzielle Sicherheitslücken in ihren Produkten und Diensten ernst. Diese Coordinated Vulnerability Disclosure Policy beschreibt, wie Schwachstellen gemeldet werden können, welche Regeln für Sicherheitsforschung gelten und wie wir gemeldete Schwachstellen bearbeiten und veröffentlichen.

1. Zweck

Ziel dieser Policy ist es, Sicherheitsforschenden, Kunden, Partnern und sonstigen Hinweisgebenden einen klaren und verantwortungsvollen Weg zur Meldung potenzieller Schwachstellen bereitzustellen. Wir wollen Risiken für Nutzerinnen und Nutzer reduzieren, geeignete Abhilfemaßnahmen vorbereiten und Informationen über Schwachstellen kontrolliert und verantwortungsvoll kommunizieren. Diese Policy begründet keinen Anspruch auf eine Vergütung, ein Bug-Bounty oder sonstige Gegenleistung und begründet keine vertraglichen Rechte zugunsten meldender Personen.

2. Geltungsbereich

Diese Policy gilt für die von der Software-Schmiede Vogler & Hauke GmbH bereitgestellten, entwickelten oder betriebenen unterstützten Produkte und Dienste im Zusammenhang mit Professional ERP. Dazu gehören insbesondere:

- Professional ERP (On-Prem)
- Lizenzserver
- MDE Web-Service
- Call-Sync
- CRM Sync
- MDE App
- PZE App
- PZE Cloud-Service

Diese Policy gilt auch für Schwachstellen in Open-Source-Komponenten und sonstigen Drittkomponenten, soweit diese in den oben genannten Produkten oder Diensten enthalten sind und sich auf deren Sicherheit auswirken können.

Nicht vom Geltungsbereich dieser Policy erfasst sind reine Drittanwendungen oder Fremdkomponenten, die nicht von der Software-Schmiede Vogler & Hauke GmbH entwickelt, gepflegt oder betrieben werden. Dazu zählen insbesondere TeamViewer, Ghostscript für den PDF-Druck sowie sonstige Drittanwendungen.

3. Meldung von Schwachstellen

Potenzielle Schwachstellen können an folgende Kontaktadresse gemeldet werden:

- E-Mail: security@softwareschmiede.com

Eine verschlüsselte Übermittlung per PGP ist derzeit nicht vorgesehen und wird nach Bereitstellung eines geeigneten Schlüssels ergänzt.

4. Inhalt einer Schwachstellenmeldung

Damit wir eine Meldung effizient prüfen und bearbeiten können, sollten nach Möglichkeit folgende Angaben enthalten sein. Ergänzung: Wenn nicht alle der nachfolgenden Angaben gemacht werden können, kann sich die Bearbeitungszeit verlängern.

- betroffene Produkte, Komponenten und Versionen
- betroffene Umgebung, Installation oder Konfiguration
- technische Beschreibung der Schwachstelle
- nachvollziehbare Schritte zur Reproduktion
- erwartetes und tatsächlich beobachtetes Verhalten
- mögliche Auswirkungen aus Sicht der meldenden Person
- vorhandene Proof-of-Concepts, Screenshots oder Logauszüge, soweit erforderlich und angemessen
- Kontaktdaten für Rückfragen
- Angabe, ob eine namentliche Nennung als Hinweisgeberin oder Hinweisgeber gewünscht ist

5. Unsere Reaktionszeiten

Wenn eine Meldung im Einklang mit dieser Policy erfolgt, streben wir folgende Reaktionszeiten an:

- Eingangsbestätigung innerhalb von 3 Werktagen
- erste fachliche Bewertung innerhalb von 10 Werktagen
- Status-Updates mindestens alle 30 Kalendertage, solange die Bearbeitung andauert
- koordinierte Offenlegung mit einem Zielwert von 90 Tagen ab Eingang einer hinreichend aussagekräftigen Meldung

In begründeten Fällen (z.B. komplexe Ursachenanalyse, Abhängigkeiten zu Dritten, koordinierte Multi-Vendor-Fälle) kann sich der Offenlegungszeitpunkt verschieben. In diesem Fall stimmen wir das weitere Vorgehen mit der meldenden Person ab.

6. Koordinierte Offenlegung

Wir behandeln Schwachstellenmeldungen nach dem Prinzip der koordinierten Offenlegung:

- Wir validieren die Meldung, bewerten Risiken und planen erforderliche Abhilfemaßnahmen.
- Wir informieren die meldende Person über den Bearbeitungsstand, solange die Schwachstelle noch nicht öffentlich bekannt ist.
- Wir veröffentlichen Informationen zu Schwachstellen grundsätzlich erst, nachdem wir eine geeignete Korrekturmaßnahme, ein Update oder eine Mitigation bereitstellen können oder eine abgestimmte Risikokommunikation erfolgt ist.
- Wir stimmen Zeitpunkt und Umfang der Veröffentlichung nach Möglichkeit mit der meldenden Person ab.

Sobald eine relevante Schwachstelle bestätigt und eine geeignete Abhilfe oder Mitigation verfügbar ist, veröffentlichen wir bei Bedarf eine Sicherheitsmitteilung oder ein Security Advisory, um betroffene Kunden und Nutzerinnen und Nutzer zu informieren. Im Falle abweichender Vorstellungen über Zeitpunkt oder Inhalt einer Veröffentlichung liegt die finale Entscheidung bei der Software-Schmiede Vogler & Hauke GmbH.

7. Regeln für Sicherheitsforschende

Wir begrüßen verantwortungsvolle Sicherheitsforschung im Rahmen dieser Policy. Dabei gelten folgende Regeln:
Erlaubt sind insbesondere:

- Tests, die darauf abzielen, Schwachstellen nachvollziehbar nachzuweisen
- Tests, die die Verfügbarkeit unserer Systeme nicht beeinträchtigen
- Tests, die keine unbefugte Offenlegung oder Veränderung von Daten bewirken
- Tests, die keine dauerhaften Veränderungen an Systemen verursachen

Nicht zulässig sind insbesondere:

- Denial-of-Service-Tests oder andere Maßnahmen, die Verfügbarkeit, Stabilität oder Integrität von Systemen beeinträchtigen können
- Social Engineering, Phishing, Täuschung oder physische Angriffe
- unautorisierter Zugriff auf Daten Dritter oder auf Konten anderer Personen
- Datenexfiltration, dauerhafte Persistenz, Malware-Einsatz oder das gezielte Ausnutzen einer Schwachstelle über das zum Nachweis Erforderliche hinaus
- Veränderungen, Löschungen oder Manipulationen von Produktivdaten
- automatisierte Massenanfragen oder Scans mit unangemessener Belastung der Infrastruktur

Meldende verpflichten sich, Informationen über die Schwachstelle bis zur abgestimmten Offenlegung vertraulich zu behandeln und nicht an Dritte weiterzugeben.

8. Safe Harbor

Wenn eine Schwachstelle nach Treu und Glauben, in Übereinstimmung mit dieser Policy und ohne Beeinträchtigung von Verfügbarkeit, Vertraulichkeit oder Integrität über das zum Nachweis Erforderliche hinaus gemeldet wird, beabsichtigen wir grundsätzlich nicht, rechtliche Schritte wegen dieser Sicherheitsforschung einzuleiten.
Dies gilt nur, wenn die meldende Person:

- die Schwachstelle unverzüglich und vertraulich meldet
- keine Daten unbefugt einsieht, speichert, verändert oder weitergibt
- keine Betriebsunterbrechung verursacht
- keine Social-Engineering- oder Täuschungsmethoden einsetzt
- nicht gegen geltendes Recht verstößt
- keine finanziellen Forderungen als Voraussetzung für die Meldung stellt
- angemessen mit uns zusammenarbeitet, um die Schwachstelle zu prüfen und zu beheben

Diese Safe-Harbor-Regelung gilt nicht für Handlungen, die über den hier beschriebenen Rahmen hinausgehen. Die Safe-Harbor-Regelung stellt keine rechtsverbindliche Zusicherung gegenüber Dritten (z.B. Strafverfolgungsbehörden, Gerichten, sonstigen betroffenen Personen oder Unternehmen) dar. Gesetzliche Rechte und Pflichten bleiben unberührt.

9. Schwachstellen in Open-Source- und Drittkomponenten

Wenn eine gemeldete Schwachstelle eine in unseren Produkten verwendete Open-Source-Komponente oder sonstige Drittkomponente betrifft, gehen wir wie folgt vor:

- Wir prüfen anhand unserer Software-Stücklisten (SBOM) und Abhängigkeitsanalysen, in welchen Produkten, Versionen oder Deployments die Komponente enthalten ist und ob die Schwachstelle in unseren Konfigurationen ausnutzbar ist.
- Wir priorisieren die Schwachstelle nach Schweregrad und Betroffenheit.
- Wir nehmen bei Bedarf Kontakt mit dem jeweiligen Open-Source-Projekt oder Drittanbieter auf und stimmen die weitere Vorgehensweise ab.
- Wir integrieren verfügbare Upstream-Fixes oder andere geeignete Abhilfemaßnahmen in unsere Produkte.
- Wir informieren betroffene Kunden und Nutzerinnen und Nutzer, wenn dies erforderlich ist.

Für Open-Source-Projekte nutzen wir bevorzugt die vom Projekt vorgesehenen vertraulichen Meldewege (z.B. Security-Advisory-Funktionen oder dedizierte Security-Kontakte). Soweit die Behebung einer Schwachstelle von Upstream-Fixes oder Updates Dritter abhängt, können wir keine bestimmte Frist für die Verfügbarkeit einer Korrekturmaßnahme zusagen.

10. Vertraulichkeit und Datenschutz

Wir behandeln alle eingehenden Schwachstellenmeldungen vertraulich. Zugriff auf Details zu gemeldeten Schwachstellen erhalten nur Personen, die diese Informationen für Prüfung, Behebung oder Freigabe benötigen.
Personenbezogene Daten, die im Rahmen einer Schwachstellenmeldung übermittelt werden, verarbeiten wir ausschließlich zum Zweck der Prüfung und Behebung der Schwachstelle sowie zur Kommunikation mit der meldenden Person. Weitere Informationen zum Datenschutz finden sich in unserer Datenschutzerklärung.

- Datenschutz: https://softwareschmiede.com/datenschutz/
- Impressum: https://softwareschmiede.com/impressum/

11. Anerkennung von Meldenden

Wenn eine Schwachstelle nachvollziehbar, relevant und im Sinne dieser Policy verantwortungsvoll gemeldet wurde, können wir die meldende Person auf Wunsch in einem Security Advisory oder an anderer geeigneter Stelle namentlich nennen. Eine solche Nennung erfolgt nur mit ausdrücklicher Zustimmung der betreffenden Person.

12. Veröffentlichung und Aktualisierung

Diese Policy gilt ab dem Zeitpunkt ihrer Veröffentlichung. Wir passen sie bei Bedarf an, insbesondere wenn sich Produkte, Prozesse, Kontaktwege oder rechtliche Anforderungen ändern. Aktualisierte Fassungen werden über dieselbe URL bereitgestellt.