Richtlinie zur Offenlegung von Schwachstellen

Cybersecurity hat für uns eine hohe Priorität. Die Sicherheit unserer Produkte und Komponenten ist ein wesentlicher Bestandteil unseres Qualitätsanspruchs. Trotz sorgfältiger Entwicklung, Tests und Qualitätssicherungsmaßnahmen können Sicherheitslücken nicht vollständig ausgeschlossen werden.

Wir begrüßen daher Hinweise auf potenzielle Schwachstellen und unterstützen eine verantwortungsvolle, koordinierte Offenlegung (Coordinated Vulnerability Disclosure). Durch Ihre Meldung helfen Sie uns, die Sicherheit unserer Produkte kontinuierlich zu verbessern.

1 Welche Meldungen nehmen wir entgegen?

Wir freuen uns über Hinweise auf mögliche Schwachstellen sowie auf Sicherheitsvorfälle mit Bezug zu unseren Produkten oder Komponenten.

Hierzu zählen insbesondere Meldungen über:

- Schwachstellen in unseren Produkten mit digitalen Elementen (Software, Firmware der Hardware),
- Schwachstellen in Bibliotheken und integrierten Drittkomponenten,
- beobachtete oder vermutete Sicherheitsvorfälle, die die Cybersicherheit oder den sicheren Betrieb unserer Produkte beeinträchtigen oder beeinträchtigen könnten.

Bitte melden Sie uns möglichst Schwachstellen bzw. Sicherheitsvorfälle, die unsere Produkte, Komponenten oder die zugehörige Infrastruktur betreffen, noch nicht öffentlich bekannt sind und durch eine nachvollziehbare Beschreibung oder geeignete Nachweise belegt werden können. Reine Ergebnisse automatisierter Scans ohne zusätzliche Erläuterungen können in der Regel nicht bearbeitet werden. Nicht unter diese Richtlinie fallen allgemeine Produktfehler ohne Sicherheitsbezug, Funktionswünsche oder Supportanfragen.

2 Wie können Sie eine Schwachstelle oder einen Sicherheitsvorfall melden?

Wenn Sie eine Schwachstelle oder einen sicherheitsrelevanten Vorfall im Zusammenhang mit unseren Produkten festgestellt haben, senden Sie uns bitte eine E-Mail an: security@cetoni.de

Um eine schnelle Bearbeitung zu ermöglichen, bitten wir Sie, möglichst folgende Informationen bereitzustellen:

- betroffenes Produkt bzw. betroffene Komponente
- Produkt- oder Softwareversion
- Beschreibung der Schwachstelle bzw. Beschreibung des beobachteten Verhaltens bei Sicherheitsvorfällen (inkl. Zeitpunkt der Beobachtung)
- Schritte zur Reproduktion
- Proof of Concept (falls vorhanden)
- Einschätzung möglicher Auswirkungen
- ggf. bereits bekannte CVE-Nummer oder Referenzen

- Hinweise, ob die Schwachstelle bereits ausgenutzt wurde

Je vollständiger Ihre Angaben sind, desto schneller können wir die Meldung bewerten.

3 Unser Umgang mit Ihrer Meldung

Nach Eingang Ihrer Meldung werden wir:

- den Eingang innerhalb von 5 Arbeitstagen bestätigen,
- die Meldung auf Plausibilität und Relevanz prüfen,
- die Schwachstelle oder den Sicherheitsvorfall technisch bewerten,
- Sie bei Rückfragen kontaktieren,
- geeignete Gegenmaßnahmen entwickeln und
- betroffene Kunden sowie gegebenenfalls zuständige Behörden entsprechend den gesetzlichen Anforderungen informieren.

Während der Bearbeitung bemühen wir uns um eine angemessene Kommunikation über den Bearbeitungsstand.

4 Verantwortungsvolle Offenlegung

Wir bitten Sie:

- uns ausreichend Zeit zur Analyse und Behebung der gemeldeten Schwachstelle einzuräumen,
- Details der Schwachstelle erst nach Abstimmung mit uns oder nach Veröffentlichung einer geeigneten Gegenmaßnahme öffentlich bekannt zu geben,
- keine Maßnahmen durchzuführen, die den Betrieb unserer Systeme oder die Verfügbarkeit unserer Produkte beeinträchtigen,
- keine personenbezogenen Daten unbefugt einzusehen, zu verändern oder zu veröffentlichen.

5 Datenschutz

Personenbezogene Daten, die Sie im Rahmen Ihrer Meldung übermitteln, werden ausschließlich zur Bearbeitung Ihrer Schwachstellenmeldung verwendet und entsprechend den geltenden Datenschutzbestimmungen verarbeitet.

6 Unser Versprechen

Wir behandeln alle Meldungen vertraulich und ausschließlich zum Zweck der Bewertung und Behebung der gemeldeten Schwachstelle.

Sofern Sie im Einklang mit dieser Richtlinie handeln und nach bestem Wissen und Gewissen (Good Faith) vorgehen, werden wir keine rechtlichen Schritte aufgrund Ihrer Schwachstellenmeldung einleiten.

Wir bedanken uns ausdrücklich für Ihre Unterstützung bei der Verbesserung unserer Produktsicherheit.