

Richtlinie zur koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure)

1. Zweck

Die Sicherheit unserer Produkte ist uns wichtig. Trotz sorgfältiger Entwicklung und Prüfung lassen sich Schwachstellen nicht vollständig ausschließen. Wir bitten daher Sicherheitsforschende, Kunden, Partner und alle weiteren Personen, uns entdeckte Schwachstellen vertraulich mitzuteilen, damit wir sie beheben können, bevor sie Dritten schaden.

Diese Richtlinie beschreibt, wie Sie uns eine Schwachstelle melden, was Sie von uns erwarten dürfen und was wir von Ihnen erbitten. Sie orientiert sich an den internationalen Normen ISO/IEC 29147 und ISO/IEC 30111 sowie an den Anforderungen der Verordnung (EU) 2024/2847 (Cyber Resilience Act).

2. Geltungsbereich

Diese Richtlinie gilt für Schwachstellen in den Hardware-, Firmware- und Softwareprodukten der Pyramid Computer GmbH, insbesondere der Produktlinien Akhet, Polytouch und Faytech, einschließlich der von uns bereitgestellten Firmware und Software.

Nicht erfasst sind die Unternehmenswebsite sowie interne IT-Systeme der Pyramid Computer GmbH. [Hinweise hierzu bitte ebenfalls an die untenstehende Adresse; wir leiten sie intern weiter.]

Betrifft Ihre Feststellung eine Komponente eines Drittanbieters (z. B. Prozessor, BIOS-Basis, Betriebssystem), geben wir die Information an den jeweiligen Hersteller weiter und halten Sie, soweit möglich, über den Stand informiert.

3. So melden Sie eine Schwachstelle

Bitte senden Sie Ihre Meldung per E-Mail an:

psirt@pyramid.de

Die Adresse wird von unserem Product Security Incident Response Team (PSIRT) betreut. Meldungen können auf Deutsch oder Englisch erfolgen.

Eine Verschlüsselung der Meldung ist derzeit nicht über einen veröffentlichten Schlüssel vorgesehen. Falls Sie vertrauliche Details verschlüsselt übermitteln möchten, schreiben Sie uns zunächst eine kurze Nachricht ohne technische Einzelheiten; wir vereinbaren dann einen geeigneten Übertragungsweg.

Folgende Angaben helfen uns bei der Bearbeitung:

- betroffenes Produkt mit Typenbezeichnung und, soweit bekannt, Firmware- bzw. Softwareversion
- Beschreibung der Schwachstelle und ihrer möglichen Auswirkungen
- Schritte zur Nachvollziehung der Schwachstelle (ggf. mit Nachweis des Konzepts)
- Hinweise, ob die Schwachstelle bereits öffentlich bekannt ist oder bereits ausgenutzt wird
- Ihre Kontaktdaten für Rückfragen sowie Ihr Wunsch, ob und wie Sie bei einer späteren Danksagung genannt werden möchten

Bitte übermitteln Sie keine personenbezogenen Daten Dritter oder Kundendaten, die für die Beschreibung der Schwachstelle nicht erforderlich sind.

4. Unser Vorgehen und unsere Zusagen

Nach Eingang Ihrer Meldung gehen wir wie folgt vor:

1. Eingangsbestätigung: Wir bestätigen den Eingang Ihrer Meldung innerhalb von [3] Werktagen.
2. Ersteinschätzung: Innerhalb von [10] Werktagen teilen wir Ihnen mit, ob wir die Schwachstelle nachvollziehen konnten und wie wir sie vorläufig einstufen.
3. Bewertung: Wir bewerten den Schweregrad nach dem Common Vulnerability Scoring System (CVSS) und legen die Dringlichkeit der Behebung fest.
4. Behebung: Wir entwickeln und prüfen eine Korrektur oder eine Übergangslösung (Workaround), gegebenenfalls in Abstimmung mit den Herstellern betroffener Komponenten.
5. Statusinformation: Wir halten Sie über den Bearbeitungsstand auf dem Laufenden, mindestens jedoch alle [30] Tage.
6. Veröffentlichung: Sobald eine Korrektur verfügbar ist, informieren wir unsere Kunden über einen Sicherheitshinweis (Security Advisory) und stellen die Aktualisierung bereit.

Sicherheitsaktualisierungen stellen wir nach den Vorgaben des Cyber Resilience Act unverzüglich und ohne gesonderte Kosten bereit.

5. Koordinierte Offenlegung

Wir bitten Sie, Einzelheiten der Schwachstelle nicht zu veröffentlichen, bevor eine Korrektur verfügbar ist und unsere Kunden Gelegenheit hatten, diese einzuspielen. Als Regelfrist gelten 90 Tage ab Bestätigung Ihrer Meldung. Bei komplexen Korrekturen, etwa wenn mehrere Hersteller beteiligt sind, stimmen wir eine Verlängerung gemeinsam mit Ihnen ab.

Wird eine Schwachstelle bereits aktiv ausgenutzt, handeln wir unverzüglich und ohne Abwarten der Regelfrist. In diesem Fall sind wir nach Artikel 14 des Cyber Resilience Act zudem verpflichtet, die zuständigen Behörden (das koordinierende CSIRT und die ENISA) innerhalb kurzer Fristen zu informieren. Personenbezogene Angaben zur meldenden Person geben wir dabei nur weiter, soweit dies erforderlich oder gesetzlich vorgeschrieben ist.

6. Was wir von Ihnen erbitten

Wir bitten Sie, bei Ihrer Sicherheitsforschung die folgenden Grundsätze zu beachten:

- Handeln Sie in gutem Glauben und mit dem Ziel, die Sicherheit zu verbessern.
- Führen Sie Tests ausschließlich an Geräten durch, die Ihnen gehören oder für deren Prüfung Sie berechtigt sind. Prüfen Sie keine Systeme unserer Kunden ohne deren Zustimmung.
- Greifen Sie nicht auf mehr Daten zu, als zum Nachweis der Schwachstelle unbedingt erforderlich ist, und geben Sie solche Daten nicht weiter oder verändern sie.
- Vermeiden Sie Tests, die die Verfügbarkeit von Systemen beeinträchtigen (z. B. Denial-of-Service-Angriffe).
- Führen Sie keine Social-Engineering-Angriffe gegen unsere Beschäftigten, Kunden oder Partner durch und keine physischen Angriffe auf Standorte.
- Geben Sie uns angemessene Zeit zur Behebung, bevor Sie Informationen veröffentlichen.

7. Rechtliche Zusicherung

Wer sich bei der Suche nach Schwachstellen und deren Meldung an diese Richtlinie hält, handelt nach unserem Verständnis in gutem Glauben. Die Pyramid Computer GmbH wird in einem solchen Fall keine rechtlichen Schritte gegen die meldende Person einleiten. Diese Zusicherung gilt nicht für Handlungen, die vorsätzlich Schaden verursachen oder gegen geltendes Recht verstoßen, und sie bindet keine Dritten, insbesondere keine Kunden oder Strafverfolgungsbehörden.

8. Anerkennung

Auf Wunsch nennen wir Sie in unserem Sicherheitshinweis als Entdeckerin bzw. Entdecker der Schwachstelle. Ein Bug-Bounty-Programm oder eine finanzielle Vergütung bieten wir derzeit nicht an.

9. Sicherheitshinweise für Kunden

Veröffentlichte Sicherheitshinweise zu unseren Produkten finden Sie auf unserer Website – Unterpunkt „Produktsicherheit - Zu den Sicherheitshinweisen“

10. Datenschutz

Die im Rahmen einer Meldung übermittelten personenbezogenen Daten verarbeiten wir ausschließlich zur Bearbeitung der Meldung und zur Erfüllung unserer gesetzlichen Pflichten. Weitere Informationen entnehmen Sie unserer Datenschutzerklärung.

11. Änderungen

Wir überprüfen diese Richtlinie regelmäßig und passen sie bei Bedarf an. Die jeweils gültige Fassung ist unter dieser Adresse abrufbar.

Pyramid Computer GmbH

Bötzingen Strasse 60,
79111 Freiburg, Germany

Ihr PSIRT-Team