oerlikon

Richtlinie zur koordinierten Offenlegung von Sicherheitslücken (CVD)
(gültig ab 09/2026, Version 1.0)

1. Einleitung und Zweck

Die Oerlikon Gruppe[1] legt großen Wert auf die Sicherheit ihrer Produkte und Dienstleistungen. Wir sind davon überzeugt, dass eine koordinierte Offenlegung von Sicherheitslücken unseren Kunden und der gesamten digitalen Gemeinschaft zugutekommt. Oerlikon hat einen formellen Prozess für den Umgang mit gemeldeten Sicherheitslücken in seinem Produktportfolio und seiner IT-Infrastruktur festgelegt.

Diese Richtlinie beschreibt, wie Sicherheitsforscher und die Öffentlichkeit potenzielle Sicherheitslücken in den Produkten von Oerlikon melden können und welche Verpflichtungen wir im Gegenzug eingehen.

2. Geltungsbereich

Diese Richtlinie gilt für Sicherheitslücken in allen Produkten mit digitalen Komponenten, die unter den Marken „Oerlikon Metco“, „Oerlikon Balzers“ oder „HRSflow“ vertrieben werden.

Nicht unter diese Richtlinie fallend:

- Produkte, deren Lebenszyklus beendet ist
- Dienste von Drittanbietern, die nicht von Oerlikon betrieben werden
- Denial-of-Service (DoS) Angriffe
- Social Engineering

3. So melden Sie eine Sicherheitslücke

Um eine Sicherheitslücke zu melden, wenden Sie sich bitte an unser Sicherheitsteam:

E-Mail: productsecurity@oerlikon.com

Website: Policies | Oerlikon

Wir bevorzugen Meldungen in Englisch oder Deutsch.

Bitte melden Sie Sicherheitslücken nicht über öffentliche Ticket Systeme, soziale Medien oder Supportanfragen.

Die offizielle Verantwortung für die Meldung aktiv ausgenutzter Sicherheitslücken an die Behörden (ENISA) liegt bei Oerlikon.

4. Was sollte Ihr Bericht enthalten?

Bitte geben Sie Folgendes an:

- Betroffenes Produkt mit Namen und Seriennummer
- Art der Sicherheitslücke (z. B. Umgehung der Authentifizierung, Befehlsinjektion, unsicheres Update)
- Auswirkungen: Was könnte ein Angreifer erreichen?
- Schritte zur Reproduktion: Schritt-für-Schritt-Anleitung
- Nachweis der Ausnutzbarkeit: Code, Screenshots oder Video (optional, aber hilfreich)
- Ihre Kontaktdaten: Damit wir Sie auf dem Laufenden halten und Sie als Urheber nennen können (optional)

[1] Oerlikon Group steht für: OC Oerlikon Corporation AG, Pfäffikon, Churerstrasse 120, CH-8808 Pfäffikon SZ, Switzerland und ihre Tochtergesellschaften. https://www.oerlikon.com/en/

5. Unsere Verpflichtungen

Oerlikon verpflichtet sich zu Folgendem:

- Bestätigung innerhalb von 48 Stunden nach Eingang Ihrer Meldung
- Erste Einstufung des Schweregrads innerhalb von 5 Werktagen
- Status-Updates mindestens alle 30 Tage bis zur Behebung
- Benachrichtigung, sobald die Sicherheitslücke behoben ist
- Ihre Nennung in unserem Sicherheitshinweis, sofern Sie nicht anonym bleiben möchten

6. Safe Harbour - Sicherer Rechtsrahmen

Sicherheitsforschung, die in gutem Glauben und im Einklang mit dieser Richtlinie durchgeführt wird, ist von Oerlikon genehmigt. Wir werden keine rechtlichen Schritte gegen Personen einleiten, die:

- diese Richtlinie einhalten
- den Zugriff auf oder die Änderung von Daten vermeiden, sofern dies über das zur Demonstration der Sicherheitslücke erforderliche Maß hinausgeht
- unsere Dienste nicht absichtlich stören
- Sicherheitslücken vor ihrer öffentlichen Bekanntgabe an uns zu melden

Oerlikon betrachtet verantwortungsvolle Sicherheitsforschung als Beitrag zur Produktsicherheit.

7. Koordinierte Offenlegung

Oerlikon bittet um eine Frist von 90 Tagen ab der ersten Meldung, um Sicherheitslücken zu beheben, bevor diese öffentlich bekannt gegeben werden.

Wir werden:

- den Zeitpunkt der Bekanntgabe gemeinsam mit Ihnen festlegen
- uns bei Bedarf mit vorgelagerten Anbietern abstimmen
- Sie vor der Veröffentlichung eines Sicherheitshinweises benachrichtigen
- Sie in unserem Sicherheitshinweis namentlich erwähnen, sofern Sie dies wünschen

Sollten Sie der Ansicht sein, dass eine Sicherheitslücke aufgrund aktiver Ausnutzung schneller offengelegt werden muss, kontaktieren Sie uns bitte, bevor Sie die Angelegenheit öffentlich machen.

Nachdem das Problem erfolgreich analysiert wurde und sofern eine Korrektur zur Behebung der Sicherheitslücke erforderlich ist, werden entsprechende Korrekturen entwickelt und für die Verteilung vorbereitet. Oerlikon wird die bestehenden Verfahren zur Kundenbenachrichtigung nutzen, um die Veröffentlichung von Patches zu verwalten. Dies kann eine direkte Benachrichtigung der Kunden oder die Veröffentlichung eines Sicherheitshinweises mit allen erforderlichen Informationen auf der Oerlikon-Website umfassen (siehe Abschnitt „Kontak Informationen“).

Oerlikon stellt Sicherheitsupdates mindestens für die neueste kompatible Version des Betriebssystems bereit. Dies gilt für den Supportzeitraum von mindestens fünf Jahren nach der erstmaligen Markteinführung.

Ein Oerlikon Security-Hinweis enthält in der Regel folgende Informationen:

• Beschreibung der Sicherheitslücke, wenn möglich mit CVE-Referenz und CVSS-Score
• Angaben zu den bekannten betroffenen Produkten und Software-/Hardwareversionen
• Informationen zu Abhilfemaßnahmen und Workarounds
• Angaben dazu, wo Korrekturen verfügbar sind
• Mit Zustimmung des Meldenden wird dessen Beitrag zur Meldung und Zusammenarbeit gewürdigt.