Coordinated Vulnerability Disclosure (CVD) Policy

(valid from 09/2026, Version 1.0)

1. Introduction and Purpose

Oerlikon Group[1] is committed to the safety and security of its products and services. We believe that coordinated vulnerability disclosure benefits our customers and the broader digital community. Oerlikon has formalized a process for handling reported security vulnerabilities in its product portfolio and IT infrastructure.

This policy describes how security researchers and the public can report potential security vulnerabilities in Oerlikon´s products, and the commitments we make in response.

2. Scope

This policy applies to vulnerabilities in any product with digital element sold under the brands “Oerlikon Metco”, “Oerlikon Balzers” or “HRSflow”.

Out of scope:

- Products that have reached end-of-life
- Third-party services not operated by Oerlikon
- Denial-of-service attacks
- Social engineering

3. How to report a vulnerability

To report a security vulnerability, contact our security team:

Email: **productsecurity@oerlikon.com**

Website: Policies on Sustainable Operations | Oerlikon

We prefer reports in English or German.

Do not report security vulnerabilities through public issue trackers, social media, or support tickets.

The official reporting responsibility for actively exploited vulnerabilities to the authorities (ENISA) lies within Oerlikon.

4. What to include in your report

Please include:

- Affected product with name and serial number
- Vulnerability type (e.g. authentication bypass, command injection, insecure update)
- Impact: What could an attacker achieve?
- Reproduction steps: Step-by-step instructions
- Proof of concept: Code, screenshots, or video (optional but helpful)
- Your contact details: So we can update you and credit you (optional)

[1] Oerlikon Group means: OC Oerlikon Corporation AG, Pfäffikon, Churerstrasse 120, CH-8808 Pfäffikon SZ, Switzerland and its subsidiaries. https://www.oerlikon.com/en/

5. Our Commitments

Oerlikon commits to:

- acknowledgment within 48 hours of receiving your report
- initial severity assessment within 5 business days
- status updates at least every 30 days until resolved
- notification when the vulnerability is patched
- credit in our security advisory unless you prefer anonymity

6. Safe Harbour

Security research conducted in good faith and in accordance with this policy is authorised by Oerlikon. We will not pursue legal action against individuals who:

- comply with this policy
- avoid accessing or modifying data beyond what is necessary to demonstrate vulnerability
- do not intentionally disrupt our services
- report vulnerabilities to us before public disclosure

Oerlikon views good-faith research as a contribution to product security.

7. Coordinated Disclosure

Oerlikon requests 90 days from initial report to address vulnerabilities before public disclosure.

We will:

- work with you on disclosure timing
- coordinate with upstream vendors if required
- notify you before publishing any security advisory
- credit you in our advisory if you wish

If you believe vulnerability requires faster disclosure due to active exploitation, please contact us before proceeding publicly.

After the issue was successfully analyzed and if a fix is necessary to cope with the vulnerability, corresponding fixes will be developed and prepared for distribution. Oerlikon will use existing customer notification processes to manage the release of patches, which may include direct customer notification, or public release of a security advisory containing all necessary information on the Oerlikon website (see section “Contact Information”).

Oerlikon will provide security updates at least for the latest compatible version of the operating system. This is valid for the support period of at least 5 years after the initial placing on the market.

An Oerlikon Security Advisory usually contains the following information:

- Description of the vulnerability, if feasible with CVE reference and CVSS score
- Identity of known affected products and software/hardware versions
- Information on mitigating factors and workarounds
- The location of available fixes
- With the reporting party’s consent, credit is provided for reporting and collaboration.