



DOMEL, d.o.o.
Otoki 21
4228 Zelezniki, Slovenia
T: +386 (0)4 51 17 100
E: info@domel.com
www.domel.com

COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY DOMEL Ltd.

Purpose: Domel supports the responsible reporting and coordinated handling of security vulnerabilities to protect users, products, and related services.

Scope: Applies to products with digital elements, firmware, software, communication interfaces, and related digital services.

Reporting: Send reports to psirt@domel.com. Anonymous submissions are accepted. Reports may be submitted in Slovenian or English.

Report contents: product/model, HW/FW/SW version, vulnerability description and impact, reproduction steps, proof of concept (if available), public disclosure status, and optional contact details.

Handling process: acknowledgement within 3 business days, initial assessment within 10 business days and remediation as quickly as possible.

Coordinated disclosure: please do not publish vulnerability details before a fix is released or an agreed disclosure date.

Good-faith principle: Domel will not take legal action against individuals acting in good faith and in accordance with this policy.

Security advisories: <https://www.domel.com/about-us/domel-product-security-incident-response-team>

PSIRT contact: psirt@domel.com