ARGUS SECURITY
intelligent fire solutions

Orama group

Vulnerability Disclosure Policy

A.8.8.1

Rev. 20260911 dated 11/09/2026

This policy applies to vulnerabilities identified in Argus Security products with digital elements, associated cloud services, customer-facing web applications, APIs, mobile applications, firmware, and supporting infrastructure owned, operated, or maintained by Argus Security.

In-scope reports concern vulnerabilities that could affect the confidentiality, integrity, availability, security, or resilience of Argus Security products, services, systems, customer data, or users.

Excluded activities: social engineering, phishing, physical security testing, denial-of-service testing, destructive testing, attempts to access or modify customer data, and testing of third-party systems not controlled by Argus Security.

Where a vulnerability concerns a third-party component used in an Argus Security product or service, Argus Security will assess the report and coordinate activities with the supplier, maintainer, customer, competent authority, CSIRT, or other appropriate party.

A security vulnerability is a weakness in our systems or services that could compromise their security. Responsibility for this policy lies with the Product Security Incident Response Team, which will review it annually.

Reporting Vulnerabilities

If you believe you have discovered a vulnerability or wish to report a security incident, please notify us using the online Vulnerability Disclosure form available in the footer of the Argus Security website.

1. We will acknowledge receipt of the report within 24 hours.
2. We ask the reporter to keep communications confidential.
3. We will work with you to understand and investigate the vulnerability.
4. We will provide a resolution timeframe in accordance with applicable legislation and the EU Cyber Resilience Act.
5. We will inform you once the vulnerability has been resolved.
6. We will publicly disclose the vulnerability in the release notes and make the required notifications.
7. The release notes may include an acknowledgement of the reporter, unless anonymity is requested.

We also ask security researchers to provide sufficient details, preferably including CVSS v3.1 or v4.0 scores; not to modify or delete data; not to carry out social engineering activities; and, where they act in accordance with this policy, Argus Security will not take legal action against them.