COMAS

a coesia company

Coordinated Vulnerability Disclosure Policy

COMAS
a coesia company

Coordinated Vulnerability Disclosure Policy

Index

1. Purpose 3
2. Applicability 3
   2.1 Revision and Date of Application
3. Reference Documents 3
4. Definitions 3
5. General Principles 4
6. Vulnerability Reporting 5
   6.1 How to Report a Vulnerability
   6.2 Contents of the Vulnerability Report
7. Vulnerability analysis and remediation 5
   7.1 Product security software updates
8. Disclosuring information on vulnerabilities 7
9. Permitted and forbidden behavior 7
   9.1 Permitted behavior
   9.2 Forbidden behavior
10. Acknowledgment of a person reporting a vulnerability 8
11. Updates to the Coordinated Vulnerability Disclosure Policy 8

Date of release: 11/09/2026

1. Purpose

Purpose of this Coordinated Vulnerability Disclosure Policy is to describe how COMAS S.p.A. receives, manages and discloses the vulnerabilities of products with digital elements manufactured by COMAS S.p.A..

2. Applicability

The provisions outlined in this Coordinated Vulnerability Disclosure Policy apply to products with digital elements manufactured by COMAS S.p.A. and falling within the scope of Regulation (EU) 2024/2847.

2.1 Revision and Date of Application

This Coordinated Vulnerability Disclosure Policy is Revision 0 and shall enter into force on 11 September, 2026.

3. Reference Documents

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024, concerning horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) 168/2013 and (EU) 2019/1020, and Directive (EU) 2020/1828 (Cyber Resilience Regulation).
- UNI CEI EN ISO/IEC 29147:2020: Information technology. Security techniques. Vulnerability disclosure.

4. Definitions

- *Product with digital elements:* Any software or hardware product and related remote data processing solutions, including software or hardware

components, placed on the market separately. For the sake of brevity, the term "product" will be used hereinafter.

- *Vulnerability:* A weakness, susceptibility, or defect in ICT products[1] or services that can be exploited by a cyber threat.
- *Exploitable vulnerability:* Vulnerability that can be used effectively by an attacker under practical operating conditions.
- *Actively exploited vulnerability:* Vulnerability with reliable evidence that an attacker exploited it in a system, without the system owner's authorization.
- *Incident:* Event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, computer and network systems[2].
- *Severe incident:* An incident having an impact on the security of the product with digital elements shall be considered severe where[3]:
  - It negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or
  - It has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

5. General Principles

COMAS S.p.A. recognizes the value of working together with the cyber security research community and with the users of products manufactured by COMAS S.p.A., and undertakes to:

- Promote responsible vulnerability reporting.
- Guarantee the confidentiality of the information received.
- Handle reports with diligence, timeliness and impartiality.
- Coordinate public disclosure of vulnerabilities, where appropriate.
- Refrain from taking legal action against anyone reporting a vulnerability, acting in compliance with this Coordinated Vulnerability Disclosure Policy and the applicable laws.

[1] ICT: Information and Communication Technology.
[2] Directive (EU) 2022/2555, Article 6(6).
[3] Regulation (EU) 2024/2847, Article 14.

6. Vulnerability Reporting

6.1 How to Report a Vulnerability

COMAS S.p.A. set the following contact points in place, through which anyone can report any vulnerabilities that have emerged on the products:

- e-mail address "Product Security Incident Response Team": psirt@comastm.it,
- form accessible with the "Report a cyber incident" button, on COMAS S.p.A. company website's Home page (www.comasitaly.com).

Receipt of the report will be confirmed to the person who reported the vulnerability via e-mail within seven days.

6.2 Contents of the Vulnerability Report

A vulnerability report must contain at least the following information:

- E-mail address where the person reporting the vulnerability can be reached
- ID of the product on which the vulnerability was found, and the product version, if relevant
- Description of the vulnerability detected and the conditions in which it occurs
- Any other information useful to contextualize the conditions in which the vulnerability occurs

7. Vulnerability analysis and remediation

Vulnerabilities that have been reported to the contact points indicated in Section 6.1 are promptly analyzed by COMAS S.p.A. The analysis may show that:

- The vulnerability concerns a component integrated into the product. In this case, COMAS S.p.A. will notify to the person who reported the vulnerability that the vulnerability report was forwarded to the manufacturer of the

component concerned, and indicate any other action undertaken to mitigate the vulnerability's impact.

- The vulnerability concerns a product for which the support period has ended, In this case, COMAS S.p.A. will reply to the person who reported the vulnerability explaining that the product's support period has ended.
- No software updates or product modifications required. In this case, COMAS S.p.A. will replay to the person who reported the vulnerability, explaining why it will not affect the product's cybersecurity.
- A recall campaign is required to make the necessary changes to the product affected by the vulnerability.
- Product software updates are necessary. In this case, updates are managed according to the methods described in Section 7.1.
- The vulnerability concerns an obsolete product for which no software updates or hardware changes are possible. In this case, COMAS S.p.A. evaluates what measures can be taken to minimize the product's cybersecurity risks and, where appropriate, notifies any known product users.

The vulnerability analysis and resolution process must normally end within 30 days. If the process takes longer, the Product Security Incident Response Team will send updates on the vulnerability analysis and resolution process every 15 days (via e-mail psirt@comastm.it) to the person who reported the vulnerability by email.

7.1 Product security software updates

Based on the analyses carried out according to the methods described in Section 7, COMAS S.p.A.:

- Prepares the necessary security software updates
- Identifies the products to which the updates will apply
- Identifies the product users
- Send them an e-mail containing the software update, or instructions for downloading the software update, and for executing the software update or, alternatively, installs the software updates through remote support

8. Disclosuring information on vulnerabilities

Once a security software update is available or if a product recall campaign is required, COMAS S.p.A., through its Product Security Incident Response Team (PSIRT), shall immediately notify known purchasers and users of products affected by vulnerabilities, by means of email communications sent from the mailbox psirt@comastm.it, providing the following information:

- Unique identification code of the vulnerability report.
- Type and model of the product affected by the vulnerability, and any other useful information to uniquely identify it (e.g. version).
- Description, severity and impact of the vulnerabilities.
- Instructions on how to fix a vulnerability (e.g., installing software updates, configuring the product, product recall methods, etc.).

9. Permitted and forbidden behavior

9.1 Permitted behavior

Security testing on the system being analyses is allowed only to the extent strictly necessary to prove the existence of a vulnerability, without negatively affecting the systems, data and users.

9.2 Forbidden behavior

It is forbidden to:

- Access, modify or extract personal, confidential or sensitive data from the system not necessary to report a vulnerability.
- Compromise service availability on the system being analyzed (e.g., through denial of service attacks).
- Introduce malware into the system being analyzed.
- Copy, modify or delete data in the system being analyzed.

- Make changes to the system being analyzed.
- Repeatedly access the system being analyzed or share the login credentials to the system being analyzed with other people.
- Execute brute force attacks to gain access to a system.
- Exploit the vulnerability for purposes other than reporting.
- Publicly disclose the vulnerability without COMAS S.p.A.'s prior written authorization.

10. Acknowledgment of a person reporting a vulnerability

Without prejudice to the fact that all information received shall be processed exclusively for the purpose of managing vulnerabilities, in compliance with Regulation (EU) 2016/679 (GDPR), at COMAS S.p.A.'s sole discretion, a person reporting a vulnerability, and providing valid and compliant contributions to this Coordinated Vulnerability Disclosure Policy, may be acknowledged by:

- Being mentioned in public thank you lists, with the person's explicit authorization.
- Being mentioned in the vulnerability disclosure documents (see Section 8), with the person's explicit authorization.
- Possible access to incentive programs, where applicable.

11. Updates to the Coordinated Vulnerability Disclosure Policy

This Coordinated Vulnerability Disclosure Policy may be amended or updated at any time.
The current version is published on the Company's website, and shall be binding starting on the date of application indicated in the Coordinated Vulnerability Disclosure Policy.