CERT MBDA IT- RFC 2350

Reference : CERT-MBDA-IT_RFC2350
Date : 26/11/2025
TLP: WHITE

MBDA
MISSILE SYSTEMS

Table of contents

1. About the document

This document contains a description of the MBDA IT CERT as recommended by the RFC2350. It presents information about the team, the services offered and how to contact the MBDA IT CERT.

1.1 Date of last update

This is version 1.0 of this document, created on 26/11/2025.

1.2 Distribution list for changes

Notification of changes to this document is not carried out by the distribution list.

1.3 Where to find this document

This document can be found on the CERT MBDA IT website: https://www.mbda-systems.com/cert/it

1.4 Authenticity of the document

This document has been signed using the PGP key of the CERT MBDA IT.

1.5 Document identification

Title: CERT-MBDA-IT_RFC2350
Version: 1.0
Created/Updated date: 26/11/2025
Validity period: this document is valid providing there is no later version.

2. Contact Information

2.1 Name of the Team

Short name: MBDA IT CERT
Full name: MBDA IT CERT

2.2 Address

MBDA ITALIA S.P.A
Via Monte
Flavio, 45
00131
Roma

2.3 Time zone

Rome (CET, UTC/GMT +1; CEST, UTC/GMT +2 during daylight saving time)

2.4 Telephone Number

+39.06.87713854

2.5 Fax Number

Not available.

2.6 Other means of Communication

Not available

2.7 Email Address

cert@mbda.it

2.8 Public key and Encryption Information

PGP is used to guarantee the confidentiality and integrity of exchanges with the CERT MBDA IT.

Key identifier: 0xCD3BA657

Fingerprint : 6BB3 91FF C4F3 B1D4 ABBF 04D1 992A 55D2 CD3B A657

The public PGP key is available at this address: https://www.mbda-systems.com/cert/it and on the CIRCL PGP key server.

CIRCL : https://openpgp.circl.lu/pks/lookup?op=get&search=0xCD3BA657

2.9 Team Members

The team is composed of Cyber Security experts. No personal information on the members of the MBDA IT CERT is published in this document.

2.10 Other Information

No other information.

2.11 Contact

To contact the MBDA IT CERT, the preferred means of communication is by e-mail at cert@mbda.it. A reply will be received within working hours.

We encourage the use of encryption with the information detailed in paragraph 2.8, Public key and Encryption Information, to ensure the integrity and confidentiality of exchanges.

In case of emergency, the MBDA IT CERT can also be reached by phone with the information detailed in paragraph 2.4.

3. Charter

3.1 Mission Statement

Our service mission is to provide MBDA with a mature detection and response capability designed to mitigate the impact from threats that put our business at risk. We accomplish this by providing a highly qualified team, executing defined processes and optimizing the use of technologies.
The activities of the MBDA IT CERT are non-profit making and are financed by MBDA ITALIA S.P.A.
Working in collaboration with the Security Operation Center (SOC), CERT MBDA Italy aims to:

- Identify and monitor threats and vulnerabilities on MBDA Italy assets, activating prevention, detection and response actions.
- Acquire insider information through trusted communications with external stakeholders.
- Coordinate the management of critical cyber incidents and define risk treatment initiatives.
- Support the MBDA Italy crisis unit in case of critical attacks.
- Ensure alignment with cyber security standards and best practices to prevent incidents.

3.2 Beneficiaries

All MBDA IT entities can benefit from the support of the MBDA IT CERT.

3.3 Affiliation

The MBDA IT CERT is a private CERT of the Defence sector.

3.4 Authority

The MBDA IT CERT carries out its activities under the authority of MBDA IT as approved by the IT Managing Director in the IT CERT Mandate.

4. Policies

4.1 Types of incidents and level of intervention

The scope of action of the MBDA IT CERT covers only high-risk IT security incidents affecting MBDA Italy.
The level of intervention depends on the type and criticality of the incident, the entities affected, their number and the resources available to intervene.

4.2 Co-operation, interaction and information sharing

MBDA IT CERT is willing to share information, without breaching confidentiality requirements, with CERT networks and to join communities.

No information on incidents or vulnerabilities will be communicated to external parties without the consent of all parties involved.

Each year, the MBDA IT CERT sends its analysts to participate in cybersecurity related events.

4.3 Communication and authentication

The MBDA IT CERT encourages the use of a PGP key for email encryption. All e-mails containing confidential information must be encrypted with a PGP key.

CERT MBDA IT respects the Information Sharing Traffic Light Protocol (TLP) with the tags WHITE, GREEN, AMBER or RED.

Unencrypted phone calls, postal services or emails can be used for sharing non-sensitive information.

5. Services

5.1 Incident response

The team offers the following services:

- Critical Incident Management to handle major incidents by reducing the impact and restoring services;
- Internal consulting on Cyber Security incidents and threat analysis;
- Collaboration with external partners to strengthen Cyber Defense.

5.2 Proactive activities

The team provides the following services:

- Cyber Threat Intelligence operational (analysis on relevant threats and attackers) and strategic (defining security objectives and interventions for the Cyber Security plan);
- Training and Cyber simulations to raise awareness of Cyber Security;
- Situational Awareness to share timely information about new risks, ongoing attacks, and Cyber trends.

6. Incident Reporting Forms

Is available an incident report form.

Incident report contain the following information:

- Incident Perimeter (Description, Perimeter);
- Incident Categorization (Date and time of detection, Impact, Category);
- Incident Analysis;
- Incident Impact;
- Remediation.

7. Disclaimer of Liability

Whilst every precaution is taken in the preparation of the information, MBDA IT CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained in this document.

If you notice any error in this document, please inform us by e-mail. We will try to correct the information as soon as possible.