# CERT MBDA UK - RFC 2350

**Reference : CERT-MBDA-UK_RFC2350**

**Date : 19/10/2022**

MBDA
MISSILE SYSTEMS

# Table of Contents

# 1. About the document

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

## 1.1. Date of last update

This is version 1.1 of this document, created on 19/10/2022. Last updated 27/01/2023.

## 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 UK website: https://www.mbda-systems.com/cert/uk

## 1.4 Authenticity of the document

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

## 1.5 Document identification

Title : CERT-MBDA-UK_RFC2350
Version : 1.1
Created/Updated date: 27/01/2023
Validity period: this document is valid providing there is no later version.

# 2. Contact Information

## 2.1 Name of the Team

Short name:MBDA UK CERT
Full name: MBDA UK CERT

## 2.2 Address

MBDA UK
Six Hills Way
Stevenage
Herts
SG1 2DA

## 2.3 Time zone

UK GMT or BST (GMT+1)

## 2.4 Telephone Number

+00 44 1438 752000 (ask for the CERT-UK Team)

## 2.5 Fax Number

Not available.

## 2.6 Other means of Communication

Not available

## 2.7 Email Address

cert-uk@mbda-systems.com

## 2.8 Public key and Encryption Information

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

Key identifier: 0xdedf9d4cdaf3d96b

Fingerprint : 6AA4441816574C9327D1E181DEDF9D4CDAF3D96B

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

CIRCL : https://openpgp.circl.lu/pks/lookup?op=get&search=0xdedf9d4cdaf3d96b

## 2.9. Team Members

The team is composed of Cyber Security experts and IM support functions. No personal information on the members of the MBDA UK CERT is published in this document.

## 2.10 Other Information

No other information.

## 2.11 Contact

To contact the MBDA UK CERT, the preferred means of communication is by e-mail at cert-uk@mbda-systems.com. 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 UK 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 optimising the use of technologies.
The activities of the MBDA UK CERT are non-profit making and are financed by MBDA UK. The missions of the MBDA UK CERT include the following tasks:

- To control and monitor cybersecurity risks through a recurrent monitoring activity on the cyber threat and vulnerabilities;
- Prevent and anticipate cybersecurity incidents by steering and coordinating vulnerability management activities;
- Ensure the detection of cyber security incidents;
- Investigating, responding to and coordinating the response to cyber security incidents.

## 3.2 Beneficiaries

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

## 3.3. Affiliation

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

## 3.4. Authority

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

# 4. Policies

## 4.1 Types of incidents and level of intervention

The scope of action of the MBDA UK CERT covers all IT security incidents affecting MBDA UK.

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 UK 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 UK CERT sends its analysts to participate in cybersecurity related events.

## 4.3 Communication and authentication

The MBDA UK 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 UK 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:

- Cyber Security incident analysis
- Cyber Security incident response support and coordination
- Vulnerability response coordination.
- Crisis management and recovery support

## 5.2 Proactive activities

The team provides the following services:
- Monitoring of cybersecurity threats and vulnerabilities;
- Detection of cybersecurity incidents.

# 6 Incident Reporting Forms

We do not have an incident report form. Please report security incidents by encrypted e-mail (see 2.11 Contact).

Incident reports should contain the following information:

- Date and time of the incident (including time zone)
- What service or system were you connecting from (Source IP, ports and protocols)
- What service or system were you connecting to (Destination IP, ports and protocols)
- Type of incident;
- Details of the reporting contact (first name, last name, email, phone number, organisation, position; PGP key);
- Any other relevant information.

# 7 Disclaimer of Liability

Whilst every precaution is taken in the preparation of the information, MBDA UK 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.