

CERT Safran RFC 2350

1. Document Information

This document contains a description of the CERT Safran in accordance with RFC 2350¹ specification. It provides basic information about our team, describes its responsibilities and services offered.

1.1. Date of Last Update

This is the version 1.2 released on 15 November 2021

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available at:
<https://www.safran-group.com/media/402052/download>

1.4. Authenticating this Document

This document has been signed with the PGP key of the CERT Safran and can be found at this URL :
https://web.safran-group.com/divers/CSIRT_Safran_0x4F8545E2_public.asc

1.5. Document Identification

Title: CERT Safran RFC 2350

Version: 1.1

Document Date: 15/11/2021

Expiration: this document is valid until superseded by a later version

¹ <https://tools.ietf.org/html/rfc2350>

CERT Safran RFC 2350

2. Contact Information

2.1. Name of the Team

Short name: CERT Safran

Full name: CERT Safran

2.2. Address

CERT Safran

46 rue Camille Desmoulins

92130 Issy-Les-Moulineaux

2.3. Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4. Telephone Number

+33 6 31 24 26 27

2.5. Facsimile Number

None available

2.6. Other Telecommunication

None available

2.7. Electronic Mail Address

cert[at]safrangroup.com

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with external CSIRT / CERT.

- User ID: CERT Safran <cert@safrangroup.com>
- Key ID: 4F85 45E2
- Fingerprint: C011 1096 C46B CCE0 BEF9 9EC1 B6C9 3296 4F85 45E2

It can be retrieved from one of the usual public key servers.

2.9. Team Members

The CERT Safran representative is Nicolas LOUIS

The full list of the team members is not publicly available.

The team is made of Cybersecurity analysts.

2.10. Other Information

None

2.11. Points of Customer Contact

CERT Safran RFC 2350

CERT Safran prefers to receive incident reports via e-mail through the email address mentioned in 2.7.

Please use our PGP key to ensure integrity and confidentiality.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

CERT Safran operate during regular business hours (9:00 AM-6:00 PM from Monday to Friday).

CERT Safran RFC 2350

3. Charter

3.1. Mission Statement

The CERT Safran Team's activities are non-profit and fully financed by Safran S.A.

The CERT Safran Team operate on the IT system of his constituency.

The mission of the CERT Safran is to:

- Investigate, respond and coordinate cybersecurity incident that can affect Safran Group's asset
- Provide vulnerabilities and cyber threat intelligence report to all CERT Safran constituency
- Deploy and maintain tools related to the security incident response
- Maintains relationship with different CERTs

3.2. Constituency

Our constituency includes Safran Group and all its subsidiaries where Safran operate the IT.

3.3. Sponsorship and/or Affiliation

CERT Safran is a private CERT in the aerospace sector. It is owned, operated and financed by Safran S.A.

3.4. Authority

The CERT Safran operate with the authority delegated by the Safran CISO. The CERT Safran is responsible for coordinating the incident response and investigate artifacts for the Safran Group's assets.

CERT Safran RFC 2350

4. Policies

4.1. Types of Incidents and Level of Support

CERT Safran manages all type of cybersecurity incidents that occur, or threaten to occur, within its constituencies.

The level of support depends on the type and severity of the given security incident, the amount of affected entities, and our resources at the time.

During regular business hours (9:00 AM-6:00 PM from Monday to Friday) CERT Safran acknowledge incidents within 24 hours.

4.2. Co-operation, Interaction and Disclosure of Information

CERT Safran exchanges all necessary non-restricted information with other CSIRTs / CERTs as well as with other affected parties involved on in the incident or incident response process.

Incident or vulnerability related information would not be publicly disclosed without the agreement of all involved parties.

4.3. Communication and Authentication

CERT Safran recommend sending all information through encrypted email.

CERT Safran support the TLP (Traffic Light Protocol) in order to classify information sharing ability.

5. Services

5.1. Incident response

The CERT Safran offer the following incident response services:

- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response on site
- Crisis management
- Incident coordination
- Vulnerability analysis
- Vulnerability coordination
- Forensic analysis

5.1.1. Incident Triage

When an incident is declared to the CERT Safran a first pass of triage is performed to assess the seriousness of the impacted assets. Then the incident get a criticality note. The note can be reviewed during the incident handling and defines the priority of the treatment.

5.1.2. Incident Coordination

The incident coordination involve the following service

- Provide a quick treatment action plan after the incident's detection
- Collection of technical evidence
- Identification of the perimeter impacted by the incident
- Proposition of immediate corrective measures
- Determining the initial cause of the incident

5.1.3. Incident Resolution

At the end of an incident, CERT Safran will provide:

- Proposition long-term corrective measures
- Informal feedback to the team concerned by the incident
- A forensic investigation report, when necessary

5.2. Proactive activities

The CERT Safran offers the following proactive activities services:

- Announcements
- Threat Hunting
- Technology watch
- Cyber Threat Intelligence
- Cyber security alerts publication
- Knowledge gathering on cyber threat actors

CERT Safran RFC 2350

6. Incident Reporting Forms

CERT Safran does not have public incident reporting form.

7. Disclaimers

While every precaution are taken in the preparation of information, notifications, and alerts, CERT Safran assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.