RFC 2350 Profile

RFC 2350 – Version 1.1 – 01/09/2026

1. Document Information

This document describes the CERT / CSIRT Olerion in accordance with RFC 2350 (*Expectations for Computer Security Incident Response*).

1.1 Date of Last Update

Version 1.1 – 2026-09-01.

1.2 Distribution List for Notifications

Updates to this document are published on this page. There is no dedicated notification mailing list; clients are informed through their usual contractual channels.

1.3 Locations where this Document May Be Found

French version: https://olerion.fr/rfc-2350/
English version: https://olerion.fr/rfc-2350-en/
A PDF version (FR and EN) is available for download.

1.4 Authenticating this Document

This document is signed with the PGP key of CERT / CSIRT Olerion. The signature is provided with the PDF version (see the public key in section 2.8).

2. Contact Information

2.1 Name of the Team

CERT / CSIRT Olerion.

2.2 Address

Olerion – 127 rue de Bellevue, 92100 Boulogne-Billancourt, France.

2.3 Time Zone

Europe/Paris (UTC+1 in winter, UTC+2 during daylight saving time).

2.4 Telephone Number

+33 1 84 19 26 72.

2.5 Facsimile Number

Not applicable.

2.6 Other Telecommunication

24/7 SOC (incident on-call): +33 7 65 65 65 44.

2.7 Electronic Mail Address

cert@olerion.fr

2.8 Public Keys and Encryption Information

For any exchange of sensitive information, the use of PGP encryption is preferred. The public key and its fingerprint will be published here and are available on request at cert@olerion.fr.

PGP key fingerprint: to be published.

2.9 Team Members

The members of CERT / CSIRT Olerion are not publicly disclosed. Team leads are communicated to authorised contacts when required.

2.10 Other Information

The SOC and CERT / CSIRT Olerion are operated in France.

2.11 Points of Customer Contact and Hours of Operation

CERT / CSIRT Olerion can be reached by email and telephone, 24/7 for security incidents. Standard support is provided according to contractual commitments.

3. Charter

3.1 Mission Statement

The mission of CERT / CSIRT Olerion is to prevent, detect and handle security incidents affecting its constituency, and to support it until normal operations are restored.

3.2 Constituency

The constituency covers Olerion's clients (SMEs, mid-caps and public authorities) as well as the systems, networks, applications and data included in their contractual cyber-protection perimeter. Interventions are possible upon referral from cybermalveillance.gouv.fr.

3.3 Sponsorship and Affiliation

CERT / CSIRT Olerion is a private CSIRT, operated by Olerion, a company specialised in cyber-protection for SMEs, mid-caps and public authorities.

3.4 Authority

CERT / CSIRT Olerion operates within the contractual framework defined with the members of its constituency. It has no authority beyond this perimeter.

4. Policies

4.1 Types of Incidents and Level of Support

CERT / CSIRT Olerion handles, among others:

- ransomware and malware,
- account compromise,
- intrusions and lateral movement,
- data leaks or suspected data leaks,
- exploitation of vulnerabilities,
- suspicious activity detected by the SOC.

The level of support depends on contractual commitments and on the criticality of the incident.

4.2 Co-operation, Interaction and Disclosure of Information

CERT / CSIRT Olerion applies the FIRST Traffic Light Protocol (TLP 2.0) for information sharing: TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT and TLP:RED. Incident information is strictly confidential and is shared only with authorised parties. No information is disclosed without prior agreement, except where legally required.

4.3 Communication and Authentication

For any sensitive information, PGP encryption is preferred (see section 2.8). Correspondents may be authenticated by PGP or by calling back a known telephone number.

5. Services

5.1 Incident Response

Triage: qualification and prioritisation of incidents.
Coordination: coordination of response actions with stakeholders (the client's IT teams, vendors, hosting providers, and competent authorities where required).
Resolution: in-depth technical analysis, containment and eradication of threats, support until normal operations are restored, and post-incident follow-up.

5.2 Proactive Activities

- use of SOC alerts and correlation of security events,
- post-incident lessons learned,
- hardening recommendations,
- continuous improvement of the security posture.

6. Incident Reporting Forms

Incidents can be reported:

- by email to cert@olerion.fr,
- by telephone (24/7),
- automatically, via the detection tools monitored by the SOC.

Please provide, where possible: your contact details, a description and timestamp of the events, the systems concerned, the actions already taken and the estimated criticality. A reporting template can be provided on request.

The client undertakes to provide accurate and up-to-date information, to apply recommendations where necessary and to co-operate actively during incident handling.

7. Disclaimers

While every precaution is taken in the preparation of this document and the associated information, CERT / CSIRT Olerion cannot be held liable for any errors or omissions, nor for any damage resulting from the use of the information it contains. Incident-related data is processed in accordance with the General Data Protection Regulation (GDPR).