Fiche RFC 2350

RFC 2350 – Version 1.1 – 01/09/2026

1. Informations sur le document

Cette fiche décrit le CERT / CSIRT Olerion conformément à la RFC 2350 (*Expectations for Computer Security Incident Response*).

1.1 Date de dernière mise à jour

Version 1.1 – 01/09/2026.

1.2 Liste de distribution et notifications

Les mises à jour de ce document sont publiées sur cette page. Il n'existe pas de liste de diffusion dédiée ; les clients sont informés via leurs canaux contractuels habituels.

1.3 Emplacements où trouver ce document

Version française : https://olerion.fr/rfc-2350/
Version anglaise : https://olerion.fr/rfc-2350-en/
Une version PDF (FR et EN) est disponible en téléchargement.

1.4 Authentification de ce document

Ce document est signé avec la clé PGP du CERT / CSIRT Olerion. La signature accompagne la version PDF (voir la clé publique en section 2.8).

2. Coordonnées

2.1 Nom de l'équipe

CERT / CSIRT Olerion.

2.2 Adresse

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

2.3 Fuseau horaire

Europe/Paris (UTC+1 en hiver, UTC+2 en heure d'été).

2.4 Téléphone

+33 1 84 19 26 72.

2.5 Télécopie

Sans objet.

2.6 Autres moyens de télécommunication

SOC 24/7 (astreinte incident) : +33 7 65 65 65 44.

2.7 Adresse électronique

cert@olerion.fr

2.8 Clés publiques et chiffrement

Pour tout échange d'information sensible, l'usage du chiffrement PGP est privilégié. La clé publique et son empreinte seront publiées ici et sont disponibles sur demande à cert@olerion.fr.

Empreinte de la clé PGP : à publier.

2.9 Membres de l'équipe

Les membres du CERT / CSIRT Olerion ne sont pas divulgués publiquement. Les responsables sont communiqués aux interlocuteurs autorisés en cas de besoin.

2.10 Autres informations

Le SOC et le CERT / CSIRT Olerion sont opérés en France.

2.11 Points de contact et heures d'ouverture

Le CERT / CSIRT Olerion est joignable par email et par téléphone, 24/7 pour les incidents de sécurité. Le support standard est assuré selon les engagements contractuels.

3. Charte

3.1 Énoncé de mission

Le CERT / CSIRT Olerion a pour mission de prévenir, détecter et traiter les incidents de sécurité affectant sa communauté d'utilisateurs, et d'accompagner celle-ci jusqu'au retour à la normale.

3.2 Périmètre (constituency)

Le périmètre couvre les clients (PME, PMI, collectivités) d'Olerion ainsi que les systèmes, réseaux, applications et données inclus dans leur périmètre contractuel de cyberprotection. Des interventions sont possibles sur saisine de cybermalveillance.gouv.fr.

3.3 Parrainage et affiliation

Le CERT / CSIRT Olerion est un CSIRT privé, opéré par la société Olerion, spécialisée dans la cyberprotection des PME, PMI et collectivités.

3.4 Autorité

Le CERT / CSIRT Olerion agit dans le cadre contractuel défini avec les membres de sa communauté. Il ne dispose d'aucune autorité au-delà de ce périmètre.

4. Politiques

4.1 Types d'incidents et niveau de support

Le CERT / CSIRT Olerion traite notamment :

- rançongiciels et logiciels malveillants,
- compromission de comptes,
- intrusions et mouvements latéraux,
- fuites ou suspicions de fuite de données,
- exploitation de vulnérabilités,
- activités suspectes détectées par le SOC.

Le niveau de support dépend des engagements contractuels et de la criticité de l'incident.

4.2 Coopération, interaction et divulgation d'information

Le CERT / CSIRT Olerion applique le Traffic Light Protocol (TLP 2.0) du FIRST pour le partage d'information : TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT et TLP:RED. Les informations relatives aux incidents sont strictement

confidentielles et ne sont partagées qu'avec les parties autorisées. Aucune information n'est divulguée sans accord préalable, sauf obligation légale.

4.3 Communication et authentification

Pour toute information sensible, le chiffrement PGP est privilégié (voir section 2.8). L'authentification des correspondants peut se faire par PGP ou par rappel téléphonique sur un numéro connu.

5. Services

5.1 Réponse à incident

Triage : qualification et priorisation des incidents.
Coordination : coordination des actions de réponse avec les parties prenantes (équipes IT du client, éditeurs, hébergeurs, autorités compétentes lorsque requis).
Résolution : analyse technique approfondie, confinement et éradication des menaces, accompagnement jusqu'au retour à la normale et suivi post-incident.

5.2 Activités proactives

- exploitation des alertes issues du SOC et corrélation des événements de sécurité,
- retours d'expérience (REX) après incident,
- recommandations de durcissement,
- amélioration continue de la posture de sécurité.

6. Formulaires de signalement

Les incidents peuvent être signalés :

- par email à cert@olerion.fr,
- par téléphone (24/7),
- automatiquement, via les outils de détection supervisés par le SOC.

Merci d'indiquer, dans la mesure du possible : vos coordonnées, la description et l'horodatage des faits, les systèmes concernés, les actions déjà menées et la criticité estimée. Un modèle de signalement peut être fourni sur demande.

Le client s'engage à fournir des informations exactes et à jour, à appliquer les recommandations lorsque nécessaire et à coopérer activement lors de la gestion d'un incident.

7. Mentions légales

Bien que toute précaution soit prise dans la préparation de ce document et des informations associées, le CERT / CSIRT Olerion ne peut être tenu responsable des erreurs, des omissions, ni des dommages résultant de l'usage des informations qu'il contient. Les données relatives aux incidents sont traitées conformément au Règlement Général sur la Protection des Données (RGPD).