

CSIRT CNAF

RFC 2350
Avril 2025
Version 1.3

Table des matières

1.	Informations sur le document	4
1.1.	Date de la dernière mise à jour	4
1.2.	Emplacement où ce document peut être trouvé	4
1.3.	Authentification du présent document	4
1.4.	Identification du document	4
2.	Informations sur les contacts	5
2.1.	Nom de l'équipe	5
2.2.	Adresse	5
2.3.	Fuseau horaire	5
	CET/CEST : Europe/Paris (GMT+01:00, et GMT+02:00 pour l'heure d'été)	5
2.4.	Numéro de téléphone	5
2.5.	Numéro de télécopie	5
2.6.	Autres télécommunications	5
2.7.	Adresse de courrier électronique	5
2.8.	Clés publiques et informations sur le chiffrement	5
2.9.	Membres de l'équipe	5
2.10.	Autres informations	5
2.11.	Points de contact avec les clients	6
3.	Charte	7
3.1.	Ordre de mission	7
3.2.	Bénéficiaires	7
3.3.	Parrainage et/ou affiliation	7
	Le CSIRT CNAF est affilié au CERT Social	7
3.4.	Autorité	7
4.	Politiques	8
4.1.	Types d'incidents et niveau de soutien	8
4.2.	Coopération, interaction et divulgation d'informations	8
4.3.	Communication et authentification	8
5.	Service	9
5.1.	Réponse aux incidents	9
5.2.	Triage des incidents	9
5.3.	Coordination de l'incident	9
5.4.	Résolution de l'incident	9
5.5.	Activités proactives	9

5.6.	Management des vulnérabilités.....	9
5.7.	Analyse sur l'état de la menace	9
6.	Décharge de responsabilité	10

1. Informations sur le document

Ce document contient une description du CSIRT CNAF tel que recommandé par la RFC2350¹. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT CNAF

1.1. Date de la dernière mise à jour

Ceci est la version 1.3 de ce document édité le 07/07/2026

1.2. Emplacement où ce document peut être trouvé

Ce document peut être trouvé sur le site <https://www.caf.fr/csirt/>

1.3. Authentification du présent document

Ce document a été signé avec la clé PGP du CERT CNAF.

La clé publique PGP, l'ID et l'empreinte sont disponibles sur le site web du caf.fr à l'adresse suivante : <https://www.caf.fr/csirt/pgp>

1.4. Identification du document

Titre : RFC 2350 du CSIRT CNAF

Version : 1.3

Date de mise à jour : 30/06/2026

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

¹ <http://www.ietf.org/rfc/rfc2350.txt>

2. Informations sur les contacts

2.1. Nom de l'équipe

Nom court : CSIRT CNAF

Nom complet : CSIRT de la Caisse nationale des allocations familiales

2.2. Adresse

32 av Sibelle, 75014 Paris

2.3. Fuseau horaire

CET/CEST : Europe/Paris (GMT+01:00, et GMT+02:00 pour l'heure d'été)

2.4. Numéro de téléphone

N/A

2.5. Numéro de télécopie

N/A

2.6. Autres télécommunications

N/A

2.7. Adresse de courrier électronique

contact-csirt@cnafr.fr

2.8. Clés publiques et informations sur le chiffrement

Notre clé PGP pour les échanges :

- Identifiant de l'utilisateur : CSIRT CNAF

- ID de la clé : 0x779F5792

- Empreinte 5CF9563C806AD9FA0510F445D994404D779F5792

La clé publique PGP, l'ID et l'empreinte sont disponibles sur le site web du caf.fr à l'adresse suivante : <https://www.caf.fr/csirt/pgp>

2.9. Membres de l'équipe

L'équipe du CSIRT CNAF est composée d'experts en cybersécurité. La liste des membres n'est pas diffusée publiquement. L'identité des membres peut être communiquée au cas par cas selon la règle du besoin d'en connaître.

2.10. Autres informations

Aucune à ce jour

2.11. Points de contact avec les clients

Le CSIRT CNAF préfère recevoir les rapports d'incidents par mail
à Contact-csirt@cnafr.fr

Veuillez utiliser notre clé PGP pour garantir l'intégrité et la confidentialité.

En cas d'urgence, veuillez spécifier la balise **[URGENT]** dans le champ objet de votre e-mail.

Le CSIRT CNAF est disponible durant les heures ouvrées, soit de 9 heures à 12h30 et de 14h à 17 heures 30 du lundi au vendredi (hors jours fériés).

3. Charte

3.1. Ordre de mission

Le CSIRT CNAF est l'équipe de réponse aux incidents de sécurité informatique de toutes les caisses d'allocations familiales. Le SOC CNAF est l'acteur principal qui travaille avec le CSIRT CNAF. Son objectif est d'apporter une assistance lors du déclenchement des incidents de sécurité.

3.2. Bénéficiaires

Les organismes pouvant bénéficier de l'accompagnement du CSIRT CNAF sont les caisses d'allocations familiales de la France ainsi que le SOC de la CNAF. Le SOC de la CNAF travaille en étroite collaboration avec le CSIRT CNAF.

3.3. Parrainage et/ou affiliation

Le CSIRT CNAF est affilié au CERT Social

3.4. Autorité

Le CSIRT CNAF réalise ses activités sous l'autorité de la CNAF (Caisse National des allocations familiales)

4. Politiques

4.1. Types d'incidents et niveau de soutien

Le CSIRT CNAF fournit les services suivants :

- Pilotage technique des incidents de sécurité et communication aux directions des organismes CNAF/CAF impactés.
- Assistance à la remédiation,
- Veille sur les vulnérabilités,
- Surveillance de la menace dans les différents domaines de la cybersécurité
- Appui à la gouvernance sur tous les aspects de sensibilisation
- Relai entre le CERT-FR, le CERT Social et les organismes CAF/CNAF.
- Consolidation des statistiques d'incidentologie à l'échelle nationale.

4.2. Coopération, interaction et divulgation d'informations

Les informations relatives à un incident tels que le nom des organismes ou les détails techniques des acteurs ne sont pas publiés sans l'accord de(s) l'organisme(s) concerné(s) par l'incident.

L'information ayant reçu l'autorisation d'être partagée peut être communiquée par le CSIRT CNAF aux entités suivantes :

- CERT Social
- CERT-FR
- Tous CSIRT/CERT sectoriel français (santé, maritime...)
- L'interCERT Français
- Tout service gouvernemental (si requis par la loi Française ou dans le cadre de réquisition judiciaire)

La diffusion d'information sera partagée avec le marquage TLP défini par FIRST

4.3. Communication et authentification

Le CSIRT CNAF conseille fortement l'utilisation de canaux de communication sécurisés, en particulier pour communiquer des informations confidentielles ou sensibles. Les informations non confidentielles ou sensibles peuvent être transmises via des courriels non chiffrés à l'adresse : Contact-csirt@cnafr.fr

5. Service

5.1. Réponse aux incidents

Le CSIRT CNAF s'appuie sur un SOC qui peut le solliciter 24H/24 et 7J/7. Le SOC effectue un triage des alertes qui peut donner lieu à l'ouverture d'un incident de sécurité.

Chaque incident est traité de manière minutieuse afin d'évaluer l'impact, la chronologie et les risques complémentaires. Chaque incident donne lieu à une analyse approfondie jusqu'à sa résolution.

5.2. Triage des incidents

Le Triage des alertes est fait par le SOC CNAF. Chaque incident ouvert est ensuite pris en charge par le CSIRT CNAF pour réévaluer sa criticité. En cas de nécessité, une escalade peut être effectuée auprès des directions des organismes impactés.

5.3. Coordination de l'incident

Le CSIRT CNAF assure la coordination de l'incident entre les équipes opérationnelles SOC CNAF et les différentes entités du SI de la CNAF impactées. Ainsi le CSIRT CNAF assure le suivi de l'incident depuis son ouverture jusqu'à sa clôture. Le CSIRT CNAF est en responsabilité du traitement de l'incident.

5.4. Résolution de l'incident

Chaque incident est suivi jusqu'à sa clôture. Chaque incident donne lieu à une analyse approfondie jusqu'à sa résolution. La clôture est effectuée lorsque la menace identifiée dans l'incident est écartée.

5.5. Activités proactives

Le CSIRT CNAF mène des activités de surveillance WEB afin de détecter des fuites ou des menaces avant que leur exploitation n'ait lieu.

5.6. Management des vulnérabilités

Le CSIRT CNAF effectue une surveillance des vulnérabilités via les canaux CERT/CSIRT et travaille à la mise en œuvre d'une vision centralisée des vulnérabilités.

5.7. Analyse sur l'état de la menace

Le CSIRT CNAF effectue une veille sur l'état de la menace en échangeant avec le CERT SOCIAL et ses autres partenaires de confiance CERT/CSIRT.

6. Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT CNAF n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.