CERT Social – RFC 2350

TLP : CLEAR	CERT Social	Version : 1.0
	RFC 2350	Date : 2023-03-30

1. Références et standards

- Arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires Sociales (PSSI-MCAS)
- MITRE ATT&CK, https://attack.mitre.org/
- MITRE D3FEND, https://d3fend.mitre.org/
- STIX 2.1

2. Information

Ce document contient une description du CERT Social selon le document RFC 2350[1]. Il fournit les informations essentielles concernant le CERT Social, ses canaux de communication, son rôle et ses responsabilités.

1. Version du document

Version 1.0, mise à jour le 30 mars 2023.

2. Liste de distribution

Il n'existe aucune liste de distribution.

3. Lieu de publication du document

La version actuelle de ce document est disponible sur demande auprès du CERT Social.

4. Authenticité du document

L'authenticité de ce document peut être confirmée sur demande auprès du CERT Social.

5. Identification du document

Titre : 'CERT Social RFC 2350'

Version : 1.0

Date du document : 30 mars 2023

Expiration : Ce document est valide jusqu'à la publication d'une nouvelle version.

[1] https://www.ietf.org/rfc/rfc2350.txt

3. Contact

1. Nom

CERT Social

2. Adresse

CNAM
16, rue Papiau de la Verrie
CS 60430
49 004 ANGERS Cedex 01

3. Fuseau horaire

CET/CEST

4. Numéro de téléphone

+ 33 2 52 09 20 06

5. Numéro de fax

Non disponible.

6. Autre canal de communication

Non disponible.

7. Adresse de courrier électronique

cert@cert-social.fr

8. Clé publique et informations de chiffrement

CERT Social utilise une clé publique PGP avec les caractéristiques suivantes :

- ID: **0xB49594E2C5EBE134**
- Empreinte: **7EC6 D0BE 7288 277C DF2A 42E2 B495 94E2 C5EB E134**

La clé publique peut être récupérée à tout moment à partir des serveurs de clés publiques applicables tels que https://pgp.circl.lu/. La clé doit être utilisée chaque fois que des informations doivent être envoyées au CERT Social de manière sécurisée. Si l'utilisation de PGP n'est pas possible, veuillez contacter le CERT Social au préalable de tout envoi de données sensibles pour convenir d'un moyen de transmission de données chiffrées secondaire.

9. Composition de l'équipe

Pour des raisons de confidentialité, la liste des membres de l'équipe n'est pas publiquement diffusée. Plus d'informations sont disponibles sur demande auprès du CERT Social.

10. Autre information

Pas d'autre information.

11. Point de contact clients

Il est préférable de contacter le CERT Social par mail.

Dans les cas d'urgence, il est possible de contacter le CERT Social par téléphone.

Les heures ouvrées sont les suivantes : du lundi au vendredi, de 9h à 18h (CEST).

4. Charte

1. Mission

Le CERT Social est un CERT public dont le mandat est le suivant :

- Coordonner et faciliter la collaboration des entités suivantes sur les missions de connaissance de la menace, la gestion de la vulnérabilité, la détection de circonstance, l'investigation et réponses aux incidents critiques et majeurs :
    - La Caisse Nationale de l'Assurance Maladie (Cnam) ;
    - La Caisse nationale des allocations familiales (CNAF) ;
    - La Caisse nationale d'assurance vieillesse (CNAV) ;
    - L'Agence centrale des organismes de Sécurité sociale (ACOSS) ;
    - La Mutualité Sociale Agricole (MSA)

2. Circonscription

Le CERT Social est composé des entités suivantes :

- La Caisse Nationale de l'Assurance Maladie (Cnam) ;
- La Caisse nationale des allocations familiales (CNAF) ;
- La Caisse nationale d'assurance vieillesse (CNAV) ;
- L'Agence centrale des organismes de Sécurité sociale (ACOSS) ;
- La Mutualité Sociale Agricole (MSA)

3. Parrainage et affiliation

Le CERT Social est affilié au ministère de la santé et de la prévention.

Il entretient des contacts avec les équipes des CSIRT nationaux et internationaux.

4. Autorité

Le CERT Social agit sous l'autorité du FSSI des ministères sociaux.

5. Stratégie

1. Types d'incidents et niveau de support

Le CERT Social s'intéresse à tout type d'incidents de cybersécurité impactant son périmètre organisationnel. Il n'intervient pas directement dans le traitement de l'incident mais assure la coordination et l'information entre les organismes.

2. Coopération, échange et confidentialité de l'information

Le CERT Social a pour mission d'éviter ou de limiter les conséquences des cyberattaques pour les organismes publics du secteur santé et social.

Les missions du CERT Social sont tournées autour de la coopération et de l'échange d'information, à savoir :

- **Etre un interlocuteur fédérateur** des organismes du secteur public santé social,
- **Faciliter le partage de l'information et la coordination** afin d'empêcher ou de limiter les cyberattaques pouvant impacter les organismes de son périmètre,
- **Permettre de mutualiser des capacités de défense et de prévention contre des incidents de cybersécurité** pour les organismes de son périmètre,
- **Informer et sensibiliser** concernant les attaques qui ciblent les organismes sociaux publics

De telles actions sont positives pour le CERT Social et les parties tierces, et peuvent aider à réaliser de manière plus efficace leur devoir ainsi que la résolution d'incidents de sécurité.

De plus, le CERT Social attache une importance cruciale à la confidentialité de la donnée et au principe du besoin d'en connaitre. Le CERT Social applique le protocole Traffic Light Protocol version 2.0[2]. Dès lors, les informations seront classifiées CLEAR, GREEN, AMBER, et RED.

Le CERT Social utilise le langage STIX et les cadres de référence MITRE afin de faciliter l'échange d'information au sein des communautés cyber.

Le CERT Social opère selon le cadre légal français.

[2] https://www.cert.ssi.gouv.fr/csirt/politique-partage/

3. Communication

Le CERT Social protège les informations sensibles selon les politiques et règlementations de la France et de l'Union Européenne.

Les communications sécurisées, incluant le chiffrement et l'authentification, sont réalisées en utilisant une clé PGP ou autre moyen, selon la sensibilité et le contexte.

6. Services

Le CERT Social fournit les services suivants :

1. Faciliter la collaboration entre les entités composant le CERT Social

Le CERT Social a pour mission principale d'accompagner les entités le composant sur les fonctions suivantes, à savoir :

- Connaissance de la menace,
- Gestion des vulnérabilités,
- Appui à la réponse aux incidents majeurs concernant une ou plusieurs de ces entités

7. Formulaire de déclaration d'un incident

Le CERT Social encourage à déclarer les incidents en utilisant des courriels chiffrés avec les informations suivantes :

- Contact et information de l'organisation, avec, si possible, la clé PGP ;
- Un résumé de l'incident/urgence/crise ;
- La date et le type d'évènement ;
- La source de l'information ;
- Les systèmes affectés ;
- L'évaluation de l'impact ;
- Les détails des observations qui ont menées à la découverte de l'incident ;
- Les données techniques pertinentes ;
- Le TLP si nécessaire

8. Clause de non-responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CERT Social ne peut être tenu responsable des erreurs ou omissions, ou des dommages résultant de l'utilisation des informations fournies.