RFC 2350
CERT CRÉDIT AGRICOLE

Version en français

SOMMAIRE

1 INFORMATIONS SUR LE DOCUMENT

Ce document décrit le CERT Crédit Agricole conformément à la spécification RFC 2350[1].
Il présente de façon synthétique les responsabilités et les services du CERT Crédit Agricole.

1.1 Date de dernière mise à jour

Version 1.5 du 10 mai 2024.

1.2 Liste de diffusion des notifications

Le CERT-AG n'utilise pas de liste de diffusion pour notifier les mises à jour de ce document.

1.3 Mise à disposition du document

Le document est disponible sur le site web du CERT-AG à l'adresse www.cert-ag.com.

1.4 Authentification du document

Le document est signé par la clé PGP du CERT-AG. Il est disponible sur le site web du CERT à l'adresse suivante : www.cert-ag.com.

1.5 Identification du document

Titre : RFC 2350 CERT-AG

Version : 1.5

Date : 10/05/2024

Expiration : Ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure.

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

2 INFORMATIONS SUR LES CONTACTS

2.1 Nom de l'équipe de réponse à incident

Nom complet : CERT Credit Agricole

Nom court : : CERT-AG

2.2 Adresse postale

Crédit Agricole SA

CERT-AG

12 Place des Etats-Unis 92127 Montrouge

FRANCE

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

Ligne fixe : **+33 1 57 72 02 55**

2.5 Numéro de télécopie

Aucun

2.6 Autres modes de télécommunication

Aucun

2.7 Adresse de courrier électronique

Pour signaler un incident de sécurité ou une cybermenace visant ou impliquant des entités du groupe Crédit Agricole, veuillez nous contacter à l'adresse suivante :cert@credit-agricole.com.

2.8 Clé publique et informations sur le chiffrement

Le chiffrement par PGP est utilisé dans les échanges avec le CERT.

- User ID: CERT Credit Agricole <cert@credit-agricole.com>
- Key ID: DFB3787D
- Fingerprint: 36795976A04E80E6CEF96ADD3B954B4DDFB3787D

Cette clé est disponible sur le site www.cert-ag.com.

Elle peut être récupérée sur le serveur de clés publiques :
https://openpgp.circl.lu/pks/lookup?op=vindex&search=0x3b954b4ddfb3787d

2.9 Membres de l'équipe

Le CERT est composé d'une équipe dédiée d'analystes en sécurité IT.

Le représentant du CERT Crédit Agricole est Marc Frédéric Gomez.

La liste complète des membres de l'équipe n'est pas publique.

2.10 Autres informations

Aucune

2.11 Points de contact

Les notifications sont à envoyer par mail à l'adresse précisée au paragraphe 2.7 - Adresse de courrier électronique.

La clé pgp du CERT doit être utilisée pour garantir l'intégrité et la confidentialité des échanges.

En cas d'urgence, le point de contact téléphonique est celui indiqué au paragraphe 2.4 - Numéro de téléphone.

Tous les services du CERT fonctionnent en 24/7. Les analystes du CERT assurent une astreinte téléphonique.

3 CHARTE

3.1 Fiche de mission

Le CERT-AG a pour mission :

- De fournir des services de veille et de reporting en Cyber Threat Intelligence pour anticiper et prévenir les menaces ciblant le groupe Crédit Agricole ;
- De coordonner, d'investiguer et de traiter les incidents de cybersécurité pouvant affecter une Entités du groupe Crédit Agricole ;
- De maintenir une coopération avec les communautés de sécurité de confiance (CSIRT et CERT).

3.2 Composition

Le CERT Crédit Agricole est un CERT interne aux Entités du Groupe Crédit Agricole. Le CERT du Crédit Agricole n'opère que pour les entités du groupe Crédit Agricole et leurs filiales.

3.3 Parrainage/Affiliation

Le CERT Crédit Agricole fait partie de Crédit Agricole S.A..

3.4 Autorité

Le CERT Crédit Agricole agit sous l'autorité du CISO groupe Crédit Agricole.

Les missions du CERT sont décidées et validées par une instance représentative du Groupe Crédit Agricole.

4 POLITIQUES

4.1 Types d'Incidents et niveau de service

Le CERT assure la coordination, l'investigation et le traitement des incidents de sécurité impactant les Entités du Groupe Crédit Agricole.

Le CERT Crédit Agricole intervient sur tout incident du domaine de la sécurité ou de la cybercriminalité impactant de façon potentielle ou avérée les Entités du Groupe Crédit Agricole.

Le CERT peut être mandaté par des Entités pour des expertises spécifiques nécessitant d'accéder à des équipements, à des équipements de collaborateurs (tels que des PC ou des smartphones) ou encore à des journaux d'équipements réseau ou de sécurité.

Le niveau d'assistance proposé par CERT-AG peut dépendre du type d'incident, de l'exhaustivité des informations disponibles et des ressources disponibles pour le gérer.

4.2 Coopération, Interaction et échanges d'informations

Le CERT-AG considère la coordination opérationnelle et le partage d'informations entre les CERT, les CSIRT et les SOC comme un élément important. L'équipe échange essentiellement des retours d'expérience et des informations pertinentes pour renforcer l'efficacité de détection et de traitement d'incidents spécifiques.

Les informations échangées par le CERT-AG avec l'ensemble de la communauté de sécurité, CERT/CSIRT externes au groupe sont limitées aux informations techniques relevant de son domaine de responsabilité et strictement nécessaires. Aucune donnée propre au Groupe ou donnée personnelle n'est échangée sans le consentement explicite des personnes autorisées et concernées.

Aucun incident ou vulnérabilité ne sera divulgué publiquement sans l'accord de toutes les parties concernées. Sauf accord contraire, les informations fournies restent confidentielles.

Au niveau du Groupe, CERT-AG s'attache à échanger toutes les informations nécessaires avec les autres équipes de sécurité des Entités qui pourraient être concernées en cas de besoin.

4.3 Communication et Authentification

Le CERT Crédit Agricole recommande l'envoi d'informations par mail chiffré.

Le CERT respecte les règles Groupe Crédit Agricole en matière de confidentialité concernant l'échange et le stockage de données sensibles ou à caractère personnel.

Lors de ses échanges avec d'autres communautés sécurité, le CERT respecte les règles de confidentialité dites « TLP » pour Traffic Light Protocol.

5 SERVICES

5.1 Réponse à incident

Le CERT propose les services de réponse à incidents ci-dessous :

- Alertes et notifications
- Gestion d'incidents
- Analyse et réponse à incident
- Analyse de vulnérabilités
- Analyse de malware
- Investigations numériques
- Partage d'IOC.

5.2 Triage d'incidents

Une première évaluation est réalisée pour confirmer l'incident de sécurité et évaluer le niveau de sévérité de l'incident en fonction de la criticité des actifs impactés. Ce niveau de sévérité peut être revu lors du traitement des incidents afin d'adapter la gestion des priorités.

5.3 Coordination d'incidents

La coordination d'incidents inclut les services suivants :

- Identification des actions de confinement et de remédiation après la détection de l'incident ;
- Notification des parties prenantes dans le respect du besoin d'en connaître ;
- Organisation de la coordination entre les parties prenantes ;
- Identification du périmètre compromis ;
- Analyse technique de l'origine de l'incident ;
- Rédaction des mesures correctives en réaction aux attaques.

5.4 Résolution de l’incident

Lors de la résolution d’incident, le CERT fournit notamment :

- Des propositions d'amélioration à la suite des constats et observations pendant l’incident ;
- Les rapports d’investigation numérique réalisées.

5.5 Activités proactives

Le CERT Crédit Agricole assure une surveillance de la menace susceptible de porter atteinte aux actifs du Groupe Crédit Agricole :

- Détection des vulnérabilités sur les technologies utilisées par le Groupe ;
- Évaluation de la menace (Cyber Threat Intelligence) ;
- Détection de fuites données externes ;
- Publication de bulletins d’alertes.

6 FICHE INCIDENT TYPE

Il n‘existe pas de format de fiche incident imposé.

7 DISCLAIMER

Le CERT Crédit Agricole prend toutes les précautions nécessaires lors de la rédaction de ses rapports, ses notifications et ses alertes, sa responsabilité ne peut cependant pas être engagée en cas d'erreurs ou d'omissions, ni en cas de dommages résultant de l’utilisation des informations transmises.