RFC 2350
CERT CRÉDIT AGRICOLE

English version

INDEX

1 DOCUMENT INFORMATION 3
1.1 Date of Last Update 3
1.2 Distribution List for Notifications 3
1.3 Locations where this Document May Be Found 3
1.4 Authenticating this Document 3
1.5 Document Identification 3
2 CONTACT INFORMATION 4
2.1 Name of the Team 4
2.2 Address 4
2.3 Time Zone 4
2.4 Telephone Number 4
2.5 Facsimile Number 4
2.6 Other Telecommunication 4
2.7 Electronic Mail Address 5
2.8 Public Keys and Encryption Information 5
2.9 Team Members 5
2.10 Other Information 5
2.11 Points of Customer Contact 5
3 CHARTER 6
3.1 Mission Statement 6
3.2 Constituency 6
3.3 Sponsoring Organization / Affiliation 6
3.4 Authority 6
4 POLICIES 7
4.1 Types of Incidents and Level of Support 7
4.2 Co-operation, Interaction and Disclosure of Information 7
4.3 Communication and Authentication 7
5 SERVICES 8
5.1 Incident response 8
5.2 Incident Triage 8
5.3 Incident Coordination 8
5.4 Incident Resolution 8
5.5 Proactive activities 9
6 INCIDENT REPORTING FORMS 9
7 DISCLAIMER 9

1 DOCUMENT INFORMATION

This document contains a description of CERT Crédit Agricole in accordance with RFC 2350[1] specification.
It provides basic information about CERT Crédit Agricole and describes its responsibilities and services offered.

1.1 Date of Last Update

Version 1.5 published on 2024-05-10.

1.2 Distribution List for Notifications

There is no distribution list set to notify on modifications to this document.

1.3 Locations where this Document May Be Found

The current version of this document is available on CERT-AG website at: www.cert-ag.com.

1.4 Authenticating this Document

This document has been signed with the PGP key of CERT-AG and is available on our website: www.cert-ag.com.

1.5 Document Identification

Title : RFC 2350 CERT-AG

Version : 1.5

Date : 2024-05-10

Expiration : this document is valid until superseded by a later version.

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

2 CONTACT INFORMATION

2.1 Name of the Team

Full name : CERT Credit Agricole
Short Name : : CERT-AG

2.2 Address

Crédit Agricole SA
CERT-AG
12 Place des Etats-Unis 92127 Montrouge
FRANCE

2.3 Time Zone

CET/CEST : Europe/Paris (GMT+01:00, and GMT+02:00 Daylight saving time)

2.4 Telephone Number

+33 1 57 72 02 55

2.5 Facsimile Number

None

2.6 Other Telecommunication

None

2.7 Electronic Mail Address

To report a security incident or a cyber-threat targeting or involving Credit Agricole Group entities, please contact us at the following address: cert@credit-agricole.com.

2.8 Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-AG.

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

The public PGP key is available at www.cert-ag.com.

It can be retrieved from the following public key server:
https://openpgp.circl.lu/pks/lookup?op=vindex&search=0x3b954b4ddfb3787d

2.9 Team Members

CERT-AG Team is composed of IT security analysts.

The CERT-AG representative is Marc Frédéric Gomez.

The list of CERT-AG team's members is not publicly available.

2.10 Other Information

None

2.11 Points of Customer Contact

The preferred method to contact CERT-AG is by sending an email to the email address in section 2.7 - Electronic Mail Address.

Please use our PGP key to ensure integrity and confidentiality.

In case of emergency, the telephone contact point is indicated in section 2.4 - Telephone Number.

CERT-AG services operate 24/7. Incident Response analysts are available on on-call duty.

3 CHARTER

3.1 Mission Statement

The mandate for CERT-AG is to:

- Provide monitoring services and Cyber Threat Intelligence reports to anticipate and prevent threats targeting Crédit Agricole group;
- Investigate, respond and coordinate cybersecurity incident that may affect constituency;
- Maintain relationship with trusted security communities (CSIRT and CERT).

3.2 Constituency

The CERT Crédit Agricole is an internal CERT for Crédit Agricole Group Entities. The CERT Crédit Agricole only operates for Crédit Agricole group entities and their subsidiaries.

3.3 Sponsoring Organization / Affiliation

The CERT Crédit Agricole is part of Crédit Agricole S.A..

3.4 Authority

The CERT Crédit Agricole is under the authority of the Crédit Agricole group CISO.

The CERT's missions are decided and validated by a representative body of the Crédit Agricole Group.

4 POLICIES

4.1 Types of Incidents and Level of Support

CERT-AG coordinates, analyses and handles cybersecurity incidents targeting Entities of Crédit Agricole Group.

The CERT undertakes to follow up on any notification sent concerning its scope.

The CERT can be mandated by Entities for specific expertise requiring access to sensitive assets, to employee devices (such as PCs or smartphones) or even to network or security equipment logs.

The level of support offered by CERT-AG may depend on the type of incident, the completeness of the information available, and the resources available to handle it.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-AG considers the importance of operational coordination and information sharing between CERTs, CSIRTs and SOCs. The team essentially exchanges feedback and relevant information to strengthen the efficiency to detect and deal with specific incidents.

The information exchanged by the CERT-AG with the entire security community, CERT/CSIRT external to the group is limited to technical information within its area of responsibility and strictly necessary. No data specific to the Group or personal data is exchanged without the explicit consent of the authorized and concerned persons.

No incident or vulnerability will be disclosed publicly without the agreement of all the concerned parties. If not agreed otherwise, supplied information is kept confidential.

At a Groupwide level, CERT-AG is willing to exchange all necessary information with other Entities security teams who may be concerned on a need-to-know basis.

4.3 Communication and Authentication

The CERT-AG preferred method of communication is encrypted email.

The CERT complies with Crédit Agricole Group rules regarding confidentiality regarding the exchange and storage of sensitive or personal data.

During its exchanges with other security communities, CERT respects the confidentiality rules known as “TLP” for Traffic Light Protocol.

5 SERVICES

5.1 Incident response

The CERT-AG provides the following incident response services:

- Alerts and notifications;
- Incident handling;
- Incident Analysis and Response;
- Vulnerability analysis;
- Malware analysis;
- Forensics analysis
- IOC sharing.

5.2 Incident Triage

A first assessment is performed to confirm the security incident and to assess the severity level of the incident based on the criticality of the impacted assets. This severity level can be reviewed during incident processing in order to adapt priority management.

5.3 Incident Coordination

The incident coordination involves the following services:

- Provide containment and remediation actions after the incident's detection;
- Notification of other involved parties on a need-to-know basis;
- Coordination between stakeholder;
- Identification of the impacted perimeter;
- Identification of Root cause analysis of the incident;
- Proposition of remediation measures.

5.4 Incident Resolution

Incident resolution services include:

- Proposals for improvement following findings and observations during the incident;
- Forensic investigation report.

5.5 Proactive activities

The CERT Crédit Agricole monitors threats likely to harm Crédit Agricole Group assets:

- Vulnerability monitoring for technologies used by the Group;
- Cyber Threat Intelligence;
- Data leak exposures detection;
- Security alerts publication.

6 INCIDENT REPORTING FORMS

CERT-AG does not have public incident reporting form.

7 DISCLAIMER

CERT Crédit Agricole takes all necessary precautions when drafting its reports, notifications and alerts; however, it cannot be held liable in the event of errors or omissions, nor in the event of damage resulting from the use of the information contained within.