ACN FR CERT

RFC 2350

Date of publication	2022-10-17
Version	1.2
Author	Gabriel DIOUF
Reviewer	Christophe LONGUEPEZ

accenture

Table of Contents

1. Diffusion

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:CLEAR information may be distributed without restriction, subject to copyright controls.

2. Document Information

This document contains a description of Accenture France CERT (ACN FR CERT) as implemented by RFC 2350[1]. It provides basic information about ACN FR CERT, its channels of communication, its roles, and responsibilities.

2.1. Date of Last Update

Version 1.2 from October 17, 2022 .

2.2. Distribution List for Notifications

There is no distribution list for notifications.

2.3. Locations where this Document May Be Found

The current and latest version of this document is available from ACN FR CERT's GitHub at: https://github.com/ACNfrCERT/Files

2.4. Authenticating this Document

This document has been signed with the PGP key of ACN FR CERT. The signature is available from ACN FR CERT's GitHub at: https://github.com/ACNfrCERT/Files

2.5. Document Identification

Title: 'ACN FR CERT RFC 2350'

Version : 1.2

Document Date: 2022-10-17

Expiration: this document is valid until superseded by a later version

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

3. Contact Information

3.1. Name of the Team

ACN FR CERT: Accenture France CERT

3.2. Address

ACN FR CERT

118 Av. de France,

75013 PARIS

FRANCE

3.3. Time Zone

CET

3.4. Telephone Number

+33 78 42 65 191

3.5. Facsimile Number

None available.

3.6. Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Accenture, please contact us at: cert.france@accenture.com

3.7. Other Telecommunication

None.

3.8. Public Keys and Encryption Information

ACN FR CERT uses the following PGP key:

- ID: 0x2D1DCEDC
- Fingerprint: 0E32 CF93 47BB 99D7 3F83 993E 4BB3 84A7 2D1D CEDC

The key can be retrieved from one of the usual public key servers such as https://pgp.circl.lu/.

The key shall be used whenever information must be sent to ACN FR CERT in a secure manner.

3.9. Team Members

The team consists of IT, Cyber and Threat security analysts.

3.10. Other Information

None available.

3.11. Points of Customer Contact

The preferred method to contact Accenture France CERT is to send an email to the following address: cert.france@accenture.com

An incident response analyst on duty can be contacted at this email address during hours of operation.

Urgent cases can be reported by phone, +33 7 84 26 51 91 on a 24/7/365 basis.

ACN FR CERT's hours of operation are usually restricted to regular French business hours (Monday to Friday 09:00 to 18:00).

4. Charter

4.1. Mission Statement

Within Accenture, the Cyber-Resilience department defines and translates the security strategy in actionable plans, oversees the level of implemented security controls, detect attack attempts, responds to incidents, and establishes operational security baseline.

ACN FR CERT's main mission is to assist its customers in responding to incidents against opportunistic and intentional cyberattacks that would hamper IT assets and harm theirs interests whenever they occur.

As part of the Cyber-Resilience France department, ACN FR CERT is the unit in charge of:

- Incident response
- Digital forensics
- Malware analysis
- Threat hunting
- Threat intelligence

ACN FR CERT's activities cover prevention, detection, response, containment, eradication, recovery, and post-incident activities as depicted in the incident response cycle.

While delivering on objectives, ACN FR CERT is driven by the following values:
- ACN FR CERT strives to act in accordance with the highest standards in terms of ethics, integrity, honesty, and professionalism,
- ACN FR CERT is committed to deliver high quality services to the clients within its constituency and while responding to external parties,
- ACN FR CERT does its best to respond to security incidents as efficiently as possible within the best possible delays,
- ACN FR CERT facilitates information exchange between Accenture entities and its peers on a need-to-know basis.

4.2. Constituency

As a commercial CSIRT, ACN FR CERT provides services to its customers which HQ are in France. ACN FR CERT customers are found among private and public sector organizations.

More information can be found on the Accenture's website:
https://www.accenture.com/fr-fr/about/company-index

4.3. Affiliation

ACN FR CERT is affiliated to Accenture SAS. ACN FR CERT strives to maintain regular contacts with various national and international CSIRT, CERT, incident response and security teams whenever such communication follows Accenture's needs and communication culture.

4.4. Authority

ACN FR CERT operates under the authority of the Accenture Security France (Accenture SAS) department within the Cyber Resilience France division.

ACN FR CERT coordinates security incidents on behalf of its constituency, and only at its constituent's request. Consequently, ACN FR CERT operates under the auspices of, and with authority delegated by its constituents.

ACN FR CERT primarily acts as an advisor regarding client security teams, and is expected to make operational recommendations. Therefore, ACN FR CERT may not have any specific authority to require specifics actions. The implementation of such recommendations is not a responsibility of ACN FR CERT, but solely of those to whom the recommendations were made.

5. Policies

5.1. Types of Incidents and Level of Support

ACN FR CERT addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see section 4.4).

The level of support given by Accenture will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or services, and the ACN FR CERT resources at the time. Depending on the security incident's type, ACN FR CERT will gradually roll out its services which include incident response and digital forensics. Incidents will be prioritized according to their apparent severity and extent.

All incidents are considered normal priority unless they are labelled EMERGENCY. ACN FR CERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to ACN FR CERT as EMERGENCY, but it is up to ACN FR CERT to decide whether to uphold that status.

ACN FR CERT is committed to keep its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited. This communication will be in the form of: email alerts, or phone calls under certain circumstances.

Note that no direct support will be given to end users. They are expected to contact their Security Operation Center (SOC) for assistance. The ACN FR CERT will support the latter people.

5.2. Co-operation, Interaction and Disclosure of Information

ACN FR CERT considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar internal and external bodies, since such cooperative actions are likely to improve ACN FR CERT's efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when ACN FR CERT's cooperation is likely to enable third-party CERTs, CSIRTs and other security teams to better perform their duties and resolve incidents.

5.3. Operations

ACN FR CERT operates under the current French legal framework.

ACN FR CERT is fully compliant with the latest approved version of CSIRT Code of Practice version 2.4 as featured at https://www.trusted-introducer.org/TI-CCoP.pdf

5.4. Communication and Authentication

ACN FR CERT protects sensitive information in accordance with relevant French, European and Accenture's regulations and policies for applicable jurisdictions.

Specifically, ACN FR CERT enforces the sensitivity markings defined by originators of information communicated to ACN FR CERT ("originator control").

ACN FR CERT also recognizes and follows the FIRST TLP (Information Sharing Traffic Light Protocol) version 2.0.

Communication security, including both encryption and authentication, is achieved by using PGP or any other agreed and tested means, depending on sensitivity and context.

6. Services

6.1. Announcements

ACN FR CERT provides announcements in the form of alerts and security briefings featuring threat intelligence of different sorts, which may include, but is not limited to detected vulnerabilities, new attack tools, techniques and processes as leveraged by the threat actors, indicators of compromise, and security measures needed to protect the Information Systems of Accenture.

6.2. Alerts and Warnings

ACN FR CERT disseminates information on cyberattacks, technical disruptions, security vulnerabilities, intrusions, malware, and provides recommendations on how to tackle the resulting risk within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis. Alerts bulletins and Newsletter could be internal or external or both, in function of the information and their sensitivity.

6.3. Pre-emptive Security Controls

ACN FR CERT performs pre-emptive security controls to detect potential breaches, vulnerabilities and misconfigurations that may be leveraged by threat actors. These security controls tend to align the compliance level of various systems and applications with the existing security policies.

6.4. Development of Security Tools

ACN FR CERT develops security tools for its own use, to improve its services and support its activities as needed. These security tools can be used by other members of its constituency or by members of the larger CERT, CSIRT, SOC and broader information security community.

6.5. Intrusion Detection

ACN FR CERT leverages tools, services, and processes to detect potential intrusions related to Accenture's SOC capabilities.

6.6. Digital Forensics and Incident Response

ACN FR CERT performs digital forensics activities whenever necessary, including but not limited to endpoint forensics, memory forensics, smartphone forensics, network forensics, cloud forensics, along with the malware analysis activities, which may result from identified forensic needs.
ACN FR CERT also performs incident response for its constituency. The incident response service as developed by ACN FR CERT covers the 6 phases of the Incident Response process: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

7. Incident Reporting Forms

To report an external incident from the outside, please provide the following details to ACN FR CERT:

- contact details and organizational information such as person or organization’s name, address, and contact information,
- email address, phone number, PGP key if available,
- IP address(es), FQDN(s), and any other relevant technical element or comment,
- supporting technical elements such as logs to illustrate the issue.

Should you desire to forward any email message to ACN FR CERT, please include all relevant email headers, bodies, and attachments if possible and as allowed by the regulations, policies, and legislation under which you operate.

8. Disclaimers

ACN FR CERT will take all necessary precautions and apply its best competence and effort while preparing, notifying, and alerting about an incident.
However, ACN FR CERT will take no responsibility for errors, omissions or damages resulting from the use of the information it provides.