SECURITY FOR THE DIGITAL AGE

CSIRT-ADVENS

# RFC 2350

CSIRT-ADVENS

14/07/2020 / - / Confidentiel

# 01 RFC 2350

## 01.1 DOCUMENT INFORMATION

This document contains a description of CSIRT-Advens in accordance with RFC 2350. It provides basic information about CSIRT-Advens, channels of communication, roles, and responsibilities.

## 01.2 DATE OF LAST UPDATE

Version 1.0 – 2020/11/12

## 01.3 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

The current version of this document can be found at:

https://CSIRT.advens.fr/RFC2350/RFC2350.pdf

## 01.4 AUTHENTICATING THIS DOCUMENT

This document has been signed with the CSIRT-Advens' PGP key. See section 2.8 for more details.

## 01.5 DOCUMENT IDENTIFICATION

**Title**: "RFC 2350 CSIRT-Advens"

**Version**: 1.0

**Document Date**: November 2020

**Expiration**: This document is valid until superseded by a later version.

# 02 CONTACT INFORMATION

## 02.1 NAME OF THE TEAM

Short name: CSIRT-Advens
Long name: CSIRT-Advens

CSIRT name: CSIRT-Advens

## 02.2 ADDRESS

CSIRT-Advens
32 rue Faidherbe
59000 Lille
France

## 02.3 TIME ZONE

Time-zone: CET/CEST

## 02.4 TELEPHONE NUMBER

Phone: +**33 1 84 16 30 26** (calls are filtered, and messages are monitored)

## 02.5 FACSIMILE NUMBER

Fax: None

## 02.6 ELECTRONIC MAIL ADDRESS

csirt (at) advens (dot) fr
This is a mail monitored by the person(s) on duty for the CSIRT-Advens.

## 02.7 OTHER TELECOMMUNICATION

**Twitter**: @CERT_Advens

## 02.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP is used for functional exchanges between CSIRT-Advens and its Partners, to transfer incident reports or alerts, for example.
Fingerprint: **9B16 51F4 3A29 BFAC C03F 06F7 2088 59AF 16C7 AB39**
https://csirt.advens.fr/csirt/custom/CSIRT-Advens.asc

## 02.9 TEAM MEMBERS

The CSIRT-Advens team leader is David QUESADA. The other members of the CSIRT team are Advens security experts and consultants.

## 02.10 OTHER INFORMATION

None

## 02.11 ADDITIONAL CONTACT INFO

The preferred method to contact CSIRT-Advens is to send an e-mail to the csirt (at) advens (dot) fr address.

The mailbox is monitored actively during hours of operations.

Days/hours of Operations: 09:00 to 18:00, Monday to Friday.

CISIRT-Advens may be contacted outside of office hours, in case of emergency.

Urgent cases can be reported by phone on **+33 1 84 16 30 26**
Contacting CSIRT-Advens by phone [to report incident] should be avoided as much as possible and used for **emergencies only**.

# 03 CHARTER

## 03.1 MISSION STATEMENT

The purpose of the CSIRT is, first, to assist the customer community in implementing proactive measures to reduce the risk of computer security incidents, and second, to assist the customer community in responding to such incidents when they occur.
CSIRT-Advens will operate according to the following key values:

- Highest standards of ethical integrity
- High degree of service orientation and operational readiness
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues
- Building on, and complementing the existing capabilities in the constituents
- Facilitating the exchange of proper practices between constituents and peers
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis.

## 03.2 CONSTITUENCY

CSIRT-Advens is composed of all the customers of Advens SAS solution, with a Service Level Agreement support contract.

## 03.3 SPONSORSHIP AND/OR AFFILIATION

CSIRT-Advens is part of Advens.

CSIRT-Advens maintain relationships with various CSIRTs throughout the world, on all continents, on an as-needed basis and with the French CSIRT-FR.

## 03.4 AUTHORITY

As CSIRT-Advens is aimed to handle incident responses on customers' perimeter, CSIRT-Advens has an advisory role with local security teams and has no specific authority to require any specific action. Any recommendation which CSIRT-Advens may provide will be implemented under the direction of the customer.

# 04 POLICIES

## 04.1 TYPE OF INCIDENT AND SUPPORT LEVEL

CSIRT-Advens is generally mandated by its customers to handle any type of incident occurring within their own perimeter.

Depending on the type of security incident, CSIRT-Advens will gradually roll out its services, which include incident response and digital forensics.

CSIRT-Advens' services include reactive and proactive services:

- Alerts and warnings ;
- Incident analysis and forensics ;
- Incident response assistance and support ;
- Incident response and remediation ;
- Threat intelligence analysis and sharing.

In addition, CSIRT-Advens liaises and can rely on the expertise and knowledge provided by other Advens services.

## 04.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSIRT-Advens operates under the restrictions imposed by French laws.

All information exchanged with a customer during an incident (and after its resolution) will be handled confidentially in secure environments using encryption if necessary. CSIRT-Advens uses the Traffic Light Protocol (TLP).

CSIRT-Advens will cooperate with other Organizations in the field of Computer Security, which may help to deliver its services, especially for incident resolution. In any such exchange, CSIRT-Advens will protect the privacy of its customers through anonymisation of technical data which may be exchanged. Customers will be informed of such exchanges.

If a customer objects to the default behaviour of CSIRT-Advens, it should be specified in an initial contractual agreement or explicitly asked in the communications with CSIRT-Advens. Requiring specific behaviour may lower the quality of assistance CSIRT-Advens may provide.

## 04.3 COMMUNICATION AND AUTHENTIFICATION

For normal communication without any sensitive information, unencrypted e-mail may be used but CSIRT-Advens strongly encourage customers to use encrypted e-mail (through PGP) to exchange data with CSIRT-Advens.

# 05 SERVICES

## 05.1 PRE-EMPTIVE SECURITY MEASURES

As the CSIRT-Advens services are delivered to Advens SAS customers, CSIRT-Advens implement any technical security measure that may help to detect or block security threats, including emerging ones, into Advens tool(s), or provide information to Advens developers to do so.

## 05.2 INCIDENT RESPONSE

CSIRT-Advens is mandated by its customer to be responsible for the coordination of security incidents somehow involving customers' perimeters or to support a customer CERT in the incident response. The technical resolution of incident is operationally left to local customers' administrators with the support of CSIRT-Advens. Without being exhaustive, the following aspects are covered by CSIRT-Advens:

### 05.2.1 | INCIDENT TRIAGE

- Investigating whether an incident occurred or not
- Determining the extent of the incident.

### 05.2.2 | INCIDENT COORDINATION

- Determining the initial cause of the incident (vulnerability exploited, …).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with the appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs with customer agreement and/or with local forces.
- Composing announcements for users, if applicable.

### 05.2.3 | INCIDENT RESOLUTION

- Providing an action plan to remove the vulnerability and supporting local administrators to implement it.
- Providing an action plan and support to help securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to provide results in proportion to their cost and risk.
- Providing action plan and support to collect any evidence after the fact to be used in criminal prosecution or any disciplinary action.

## 05.3 PROACTIVE ACTIVITIES

CSIRT-Advens performs the following proactive activities:

- Technology watch
- Intrusion detection
- Development of security tools
- Sharing information about major security threats or vulnerabilities to its customers
- Training on security topics

# 06 INCIDENT REPORTING FORMS

No public form is proposed on our web site to report incident to CSIRT-Advens, but you can directly use the contact e-mail with proper information when needed (using the PGP Key). Advens subscribers can use internal tools in Advens frontend to share events and the required information.

In case of an emergency or a crisis, please provide to CSIRT-Advens the following information at least:

- Contact details and organizational information (minimal): name of the person, organization name, email address and telephone number
- IP address(es), FQDN(s), and any other relevant technical element with the associated observations
- Scan results (if any) and/or any extract from the log showing the problem

# 07 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications, and alerts, CSIRT-Advens assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.


aDvens
SECURITY FOR THE DIGITAL AGE

advens.fr

*Lille +33 3 20 68 41 81*
*Paris +33 1 84 16 30 25*
*Lyon +33 4 28 29 08 29*
*Bordeaux +33 5 35 54 82 84*