RFC 2350

OWN-CERT

CERT TEAM

•SECURITY
(SEKOIA Services)

contact:
cert@own.security

Version	1.1
TLP	TLP:CLEAR
Author	CERT-OWN
Date	20/10/2022
Reference	RFC2350
Revision note	Moving to new company name Own

1. Document Information

This document contains a description of the OWN-CERT (ex CERT-SEKOIA) in accordance with RFC 2350 specification. It provides basic information about our team, describes its responsibilities and services offered.

Distribution list for notifications

There is no distribution list for notifications.

Locations where this document may be found

The current and latest version of this document is available at: https://own.security/rfc-2350.

Authenticating this document

This document has been signed with the PGP key of the OWN CERT.

2. Contact Information

Name of the team

Short Name	OWN-CERT
Full Name	OWN Computer Emergency Response Team

Address

Paris	18 Place de la Madeleine, 75008 PARIS

Time Zone

CET/CEST: **Europe/Paris** (GMT+01:00, and GMT+02:00 on DST)

Phone Number

Phone	+33 805 69 21 42

Facsimile Number

None available.

Other Telecommunication

Online Video conferencing is available on request.

Electronic mail address

Email: cert@own.security

An alias has been create where all emails incoming to csirt@own.security are redirected to cert@own.security.

Public keys and encryption information

User ID	OWN-CERT (OWN Computer Emergency Response Team) <cert@own.security>
Key ID	0x4078F9824693BE16
Fingerprint	C17E F7F1 DC00 0EB2 CAF5 F87D 4078 F982 4693 BE16

The key and its signatures can be found at the usual large public keyservers. It can be retrieved from one of the usual public key servers.

Team members

The OWN CERT representative is Barbara LOUIS-SIDNEY (Head of CERT).

Security incidents are handled by Grégory GUILLERMIN (Lead Incident Handler).

The full list of the team members is not publicly available. The team is made of Cybersecurity analysts.

Other Information

General Information about OWN can be found on its website.

Points of customer contact

OWN-CERT prefers to receive incident reports via **e-mail** through the email address mentioned in Electronic mail address.

Please use our PGP key to ensure integrity and confidentiality.

If it is not possible (or not advisable for security reasons) to use e-mail, OWN-CERT can be reached by telephone during regular office hours as mentioned in Phone Number.

OWN-CERT's hours of operation are restricted to regular business hours (09:00-19:00 Monday to Friday except holidays).

3. Charter

Mission statement

The purpose of OWN-CERT is to assist its constituency in investigating and responding to computer security incidents when they occur. To fulfil this mission, OWN-CERT relies on DFIR expertise but also has developed skills in gathering and processing threat intelligence data.

Constituency

As a commercial CERT, OWN-CERT's constituency is its customers.

Sponsorship and/or affiliation

OWN-CERT (ex CERT-SEKOIA) is part of OWN SAS.

Authority

OWN-CERT investigates and coordinates the responses to security incidents for its constituency. However, it does not have formal authority over its constituency. It only provides support and advice.

4. Policies

Types of incidents and level of support

OWN-CERT addresses all types of computer security incidents which occur, or threaten to occur, at its constituency.

The level of support given by OWN-CERT will vary depending on the contract between OWN-CERT and the customer.

In all cases, OWN-CERT will start responding to security incidents within one business day.

Incidents are classified following the incident taxonomy available at https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf.

Co-Operation, interaction and disclosure of information

OWN-CERT considers co-operation and information sharing between CERTs as highly important.

OWN-CERT is a member of the InterCERT-FR group.

OWN-CERT complies with the French law. OWN-CERT also complies with TI CSIRT Code of Practice (CCoP v2.4) and adopted Information Sharing Traffic Light Protocol (FIRST TLP v2.0).

COMMUNICATION AND AUTHENTICATION

As far as possible, we propose encrypted data communications with our constituents:

- Information exchange can be handled by email using PGP.
- File sharing can be handled with our dedicated sharing solution using HTTPS
- Discussions can be handled on our videoconference solution using HTTPS or by phone if not too sensitive.

In case of identity doubt or technical risk for identity theft, we use a second channel to confirm the identity.

5. SERVICES

INCIDENT RESPONSE

OWN-CERT will assist its constituency in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management.

INCIDENT TRIAGE

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

INCIDENT COORDINATION

The incident coordination involves the following services:

- Organizing the means during the incident.
- Facilitating contact with other sites which may be involved.
- Tracking actions engaged during the incident.
- Listing tasks that should be distributed.
- Providing reports for follow-up activity.
- Explaining the incident to management.

INCIDENT RESOLUTION

Performing expertise tasks such as forensics analysis, network traffic analysis and malware analysis.

- Support its constituency with threat intelligence related to the incident.
- Providing support for removing the vulnerability.
- Providing support for securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.

Proactive Activities

OWN-CERT provides tailored and on-demand cyber threat intelligence services and consulting, and advanced OSINT investigations. OWN-CERT monitors and analyses cyber threats on strategic, tactical, technical and operational levels, performing the below activities:

- OWN-CERT monitors, detects and analyses malicious activities, attacks, infrastructures, tools, malware, actors and campaigns
- OWN-CERT monitors and investigate cyber-criminals' channels
- OWN-CERT performs geopolitical, sectoral, country and strategic analysis of campaigns and threat actors modus operandi

OWN-CERT provides the following threat intelligence services:

- Sectoral Threat Intelligence reports
- Reports on Requests for Intelligence or Investigations
- Exposure assessment
- Threat Intelligence Risk Reports and matrix

OWN-CERT also provides the following proactive services:

- Threat Intelligence Maturity assessment
- Purple team exercises and readiness assessments
- Training services: OWN provides trainings in the French language including "Incident First Responder", "Malware Analysis" and "Introduction to Cyber Threat Intelligence"

Security tools, available on our GitHub account Own.

6. Incident Reporting forms

OWN-CERT has a public incident reporting form OWN | Request & contact .

If possible, please provide the following information:

- Contact information, including electronic mail address and telephone number
- Date and time when the incident started
- Date and time when the incident was detected
- Incident description
- Affected assets, impact
- Actions taken so far

Incident Reporting forms

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

OWN

OWN•SECURITY