Almond

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

CERT CWATCH
RFC 2350

17.10.23

Version
1.1

Référence du document
Almond-CWATCH-CERT-RFC2350

Almond
7 avenue de la Cristallerie,
92310 Sèvres, SAS au capital
de 17 977 770,00 €
SIREN 841 059 553
TVA FR24 841 059 553

www.almond.eu

TABLE OF CONTENTS

1. DOCUMENT INFORMATION

This document contains a description of CERT CWatch Almond (CERT-CWatch) as implemented by RFC 2350.

It provides information about the CERT CWatch, how to contact the team, and describes its responsibilities and the services offered by CERT CWatch.

1.1 Date of Last Update

Version 1.1, published on 2023-10-17.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

The current and latest version of this document is available on Almond's website.

The URL is: https://almond.eu/CWATCH-RFC2350.pdf

1.4 Authenticating this Document

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

The signature is available on Almond's website.

The URL is: https://almond.eu/CWATCH-RFC2350.pdf.sig

2. CONTACT INFORMATION

2.1 Name of the Team

CERT CWatch Almond (short name CERT-CWatch)

2.2 Address

Almond – CERT CWatch

Bâtiment Crisco Duo

7 avenue de la Cristallerie

92310 Sèvres

FRANCE

2.3 Time Zone

CET/CEST

2.4 Telephone Number

+33 1 83 75 36 94 (Monday-Friday, 8 am – 7 pm CET/CEST).

2.5 Facsimile Number

None available.

2.6 Electronic Mail Address

CERT-CWatch can be contacted using the following email address:

- alerte@cwatch.almond.eu : incidents reports should be sent to this email address.
- cwatch@almond.eu : general communication.

2.7 Other Telecommunication

None available.

2.8 Public Keys and Encryption Information

CERT-CWatch PGP key is:

- Fingerprint: A885 839E 718A 7B1C 6378 7D5D 796B 16AB C3B8 02BB

The key can be retrieved from one of the usual public key servers such as:

- https://keys.openpgp.org/search?q=A885839E718A7B1C63787D5D796B16ABC3B802BB
- and https://almond.eu/CERT_ALMOND_PGP_public_key.gpg

It is associated to the general communication email address: **alerte@cwatch.almond.eu**.

This key shall be used whenever information must be sent to CERT-CWatch in a secure manner.

2.9 Team Members

CERT-CWatch team leader is Julien STEUNOU.

The team is composed of IT security analysts delivering SOC and CERT services.

2.10 Other Information

Any other information can be found on CERT-CWatch webpage:

https://almond.eu/cybersecurity/i-need-reaction/

2.11 Points of Customer Contact

The preferred method for contacting CERT-CWatch is via email using the following email address:

- alerte@cwatch.almond.eu : incidents reports should be sent to this email address.
- cwatch@almond.eu : general communication.

If it is not possible (or advisable due to security reasons) to use email, you can reach us via telephone at:

- +33 1 83 75 36 94

CERT-CWatch hours of operation are generally restricted to local regular business hours: Monday-Friday, 8 am-7 pm CET/CEST.

3. CHARTER

3.1 Mission Statement

CERT-CWatch mission is to support Almond, Amossys, Board of Cyber and Hifield group and its customers to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm their interests.

The scope of CERT-CWatch covers anticipation, protection, detection and incident response.

3.2 Constituency

CERT-CWatch's constituency is composed of:

- CERT-CWatch's paid subscribers,
- Almond,
- Amossys (sister company),
- Board of Cyber (sister company),
- Hifield (holding).

CERT-CWatch provide its services to a group of customers that are kept confidential because of the clients' contracts.

3.3 Affiliation

CERT-CWatch is affiliated to Almond, a consultancy cabinet specialized in Information Security and Digital & Technology. Funding is provided by Almond.

3.4 Authority

CERT-CWatch main purpose is the coordination of incident response. As such, we advise our constituency and have limited authority to demand certain actions.

4. POLICIES

4.1 Types of Incidents and Level of Support

CERT-CWatch is authorized to handle all types of cybersecurity incidents that would hamper the integrity or harm the interests of its constituents.

Depending on the security incident's type and its customers' contract, CERT-CWatch will gradually roll out its services which include incident response and digital forensics.

The level of support given by CERT-CWatch will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available CERT-CWatch's resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-CWatch will cooperate with other organizations in the field of computer security. This cooperation also includes and often requires the exchange of information regarding security incidents and vulnerabilities.

CERT-CWatch will protect the privacy of reporters, partners and our constituents, and therefore (under normal circumstances) pass on information in an anonymized way only unless other contractual agreements apply.

CERT-CWatch operates within the current French legal framework.

4.3 Communication and Authentication

CERT-CWatch protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU.

CERT-CWatch respects the sensitivity markings allocated by originators of information communicated to CERT-CWatch ("originator control").

CERT-CWatch also recognizes and supports the TLP (Traffic Light Protocol) version 2.0.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

5. SERVICES

CERT-CWatch offers a wide range of services to its constituents. Services may vary from one customer to another depending on the client's contract.

5.1 Anticipation

CERT-CWatch offers the following anticipation services to its constituents, along with Almond's offensive security and security governance teams:

- Cyberdefense program design
- Threat landscape assessment
- Risk management
- Security awareness and phishing test campaign
- Crisis management training
- Penetration testing and redteal
- Security rating

5.2 Protection

CERT-CWATCH offers protection managed services to cover:

- Vulnerability watch and managed vulnerability scan
- Configuration optimization of Web application firewall, IDS/IPS and EDR
- Operational threat intelligence feeds

5.3 Detection

CERT-CWatch offers a log analysis service to detect potential cyber-security incidents:

- External security watch services to detect:
  - Relevant security events targeting involving constituent's external assets,
  - Technical identity theft (domains, certificate…)
  - Data exposure over Internet
- Internal SOC services relying on log analysis service to detect potential cyber-security incidents. This log analysis service is based on standard and custom rules defined using Indicators of Compromise, geolocation databases, pattern matching, …

5.4 Reaction

CERT-CWatch will assist the IT teams of its constituents in handling the technical and organizational aspects of incidents.

Communication and incident reporting

CERT-CWatch will:

- determine whether an incident is authentic,
- assess and prioritize the incident based on its constituent's activities,

- report the incident to its constituents.

Incident Coordination and management

CERT-CWatch will:

- determine the involved IT teams inside or outside of its constituent's organizations,
- contact the involved IT teams / organizations to investigate the incident and take the appropriate steps,
- facilitate contact to other parties which can help resolve the incident,
- advise the IT teams of its constituents on appropriate actions,
- follow up on the progress of the concerned local IT teams.

Digital forensics

CERT-CWatch will perform digital forensics whenever necessary, including hard drive and memory forensics.

Malware analysis and reverse engineering

CERT-CWatch will perform malware analysis and reverse engineering whenever necessary to enrich its IoC database and share this information with its constituents and other CERTs / CSIRTs / SOCs if deemed necessary or useful to them on a need-to-know basis.

6. INCIDENT REPORTING FORMS

No local form has been developed to report incidents to CERT-CWatch.

In case of emergency or crisis, please provide CERT-CWatch at least the following information:

- contact details and organizational information – name of person and organization name and address;
- email address, telephone number;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- scanning results (if any) - an extract from the log showing the problem;
- in case you wish to forward any emails to CERT-CWatch, please include all email headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate.

7. DISCLAIMERS

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

Almond

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

THANK YOU

Contact
T. +33 1 83 75 36 94
E. cwatch@almond.eu
E. alerte@cwatch.almond.eu