TLP:WHITE

RFC 2350
CSIRT-VADE

TLP : WHITE | PUBLIC

TLP : WHITE information may be distributed freely

Version 1.0

TLP:WHITE

Table of contents

Document information

This document contains a description of CSIRT-VADE in accordance with RFC 2350[1]. It provides basic information about CSIRT-VADE, its channels of communication and its roles and responsibilities.

Date of last update

Version 1.0 – 13 June 2023

Distribution list for notifications

N/A

Locations where this document may be found

The current version of this document can be found at:

https://csirt.vadesecure.com/CSIRT_VADE_RFC2350.pdf

Authenticating this document

This document has been signed with the PGP key of CSIRT-VADE.

https://csirt.vadesecure.com/CSIRT_VADE_RFC2350.pdf.gpg

Document identification

Title: CSIRT-VADE – RFC 2350
Version: 1.0
Document Date: 13 June 2023
Expiration: this document is valid until superseded by a later version

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

Contact information

Name of the team

CSIRT-VADE

Address

PA des 4 vents
2b Avenue Antoine Pinay
59510 Hem
France

Time zone

CET/CEST

Facsimile number

03 59 61 66 50

Electronic email address

csirt@vadesecure.com

Other telecommunication

N/A

Public keys and encryption information

We use PGP for functional exchanges (notifications, incident reporting, etc.) with our peers, partners and constituents.

ID: 0xE101BD8CE069E5EE
Fingerprint: 7DE0 2E7E 2F81 D352 6261 CF7B 5A9E 841E BEBD C868

The key can be retrieved at any time from applicable public key servers such as https://pgp.circl.lu/. The key shall be used whenever information must be sent to CSIRT-VADE in a secure manner.

Team members

The team consists of email Security Analysts, Vade Security experts and CISO.

Other information

N/A

Points of contact

The preferred method to contact CSIRT-VADE is by sending an email to the following address:

csirt@vadesecure.com

A security analyst can be contacted at this email address during hours of operation.
CSIRT-VADE's hours of operation are usually restricted to regular French business hours (Monday to Friday 09:00 to 18:00).

Charter

Mission statement

Vade Threat Intelligence and Response Center team contributes to the security of electronic message mailboxes of its constituents by helping to prevent, detect, mitigate and respond to cyber-attacks that originate from this vector.

CSIRT-VADE is the team responsible for handling incident responses and conducting threat intelligence activities specifically related to malicious email campaigns.

CSIRT-VADE's primary mission revolves around ensuring the utmost accuracy of Vade Technology in securing the email businesses of its constituents.

Constituency

The constituency of CSIRT-VADE is composed of the following types:

- ISP and Telcos
- Hosting services and Email Service Providers (ESP)
- OEM

- Corporate (B2B companies)

Sponsorship and/or affiliation

CSIRT-VADE is affiliated to the Vade company (https://www.vadesecure.com) and sponsored by CERT of ADVENS (https://www.advens.fr/taxo_metier/cert/).

Authority

CSIRT-VADE operates under the authority of Vade Head of TIRC and CISO.

Policies

Types of incidents and level of support

CSIRT-VADE handles all malicious emails occurring in VADE's constituents' mailboxes.

The level of support provided by CSIRT-VADE will be contingent upon the severity of the security incident or issue, its assessed impact, and the resources available to CSIRT-VADE at the time of the incident.

Co-operation, interaction and disclosure of information

CSIRT-VADE highly 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 CSIRT-VADE's efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when CSIRT-VADE's cooperation is likely to enable third-party CERTs, CSIRTS and other security teams to better perform their duties and resolve incidents.

CSIRT-VADE operates within the current French legal framework.

Communication and authentication

To ensure communication security, which encompasses encryption and authentication, we employ PGP (Pretty Good Privacy) or other mutually agreed-upon and tested methods. The choice of encryption and authentication mechanism is determined based on the sensitivity of the information and the specific context in which it is being utilized.

Services

Announcements

CSIRT-VADE provides security bulletin about new threats and/or techniques spotted in the wild of email security.

Indicators of compromise publication

CSIRT-VADE disseminates information about compromised IP addresses or domains used against its constituents.

Education and training

CSIRT-VADE offers training focused on promoting good practices in Email Security. It aims to educate and empower individuals to enhance their understanding of email security best practices.

Analyse malicious email campaign

CSIRT-VADE offers comprehensive analysis of false negative campaigns, employing its threat intelligence capabilities. This analysis involves:

- the identification of such campaigns, leveraging the insights provided by CSIRT-VADE's threat intelligence.
- In response, CSIRT-VADE examines how VADE technology addressed the attack and prevented further similar attacks. This includes an assessment of the effectiveness of the implemented measures and how they contributed to stopping the attack.
- To ensure continuous improvement and adaptability, CSIRT-VADE closely monitors the evolving threat landscape. This allows for the ongoing adaptation of measures and protections to safeguard the interests of its constituents.

Incident reporting

No local form has been developed to report incidents to CSIRT-VADE.
To report an external incident from the outside, please provide the following details to CSIRT-VADE:

- 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, proof of concept, screenshots, or any other artefact that help our analysts processing your report.
  Should you desire to forward any email message to CSIRT-VADE, please include all relevant email headers, bodies and attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

Disclaimer

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

TLP:WHITE