RFC 2350

CSIRT HORNETSECURITY

TLP: WHITE | PUBLIC

TLP: WHITE information may be distributed freely

Version 1.0

HORNETSECURITY

Table of content

1 Document information

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

1.1 Date of last update

Version 1.0 – 07 January 2025

1.2 Distribution list for notifications

N/A

1.3 Locations where this document may be found

The current version of this document can be found at:
https://csirt.hornetsecurity.com/CSIRT-HORNETSECURITY_RFC2350.pdf

1.4 Authenticating this document

This document has been signed with the PGP key of CSIRT-HORNETSECURITY.
https://csirt.hornetsecurity.com/CSIRT-HORNETSECURITY_RFC2350.pdf.sig

1.5 Document identification

Title: CSIRT-HORNETSECURITY – RFC 2350
Version: 1.0
Document Date: 07 January 2025
Expiration: this document is valid until superseded by a later version

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

2 Contact information

2.1 Name of the team

CSIRT-HORNETSECURITY

2.2 Address

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

2.3 Time zone

CET/CEST

2.4 Facsimile number

03 59 61 66 50

2.5 Electronic email address

csirt@hornetsecurity.com

2.6 Other telecommunications

N/A

2.7 Public key and encryption information

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

Fingerprint: DC76 36AD 9BCD D4DC 087F CEA1 139C 80C0 E901 35EF

https://csirt.hornetsecurity.fr/CSIRT-HORNETSECURITY.asc

2.8 Team members

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

2.9 Other information

N/A

2.10 Points of contact

The preferred method to contact CISRT-HORNETSECURITY is by sending an email to the following address:

csirt@hornetsecurity.com

A security analyst can be contacted at this email address during hours of operation.

CSIRT-HORNETSECURITY’s hours of operation are usually restricted to regular French business hours (Monday to Friday 09:00 to 18:00).

3 Charter

3.1 Mission statement

Hornetsecurity 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-HORNETSECURITY is the team responsible for handling incident responses and conducting threat intelligence activities specifically related to malicious email campaigns.
CSIRT-HORNETSECURITY's primary mission revolves around ensuring the utmost accuracy of Hornetsecurity Technology in securing the email businesses of its constituents.

3.2 Constituency

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

- ISP and Telcos
- Hosting services and Email Service Providers (ESP)
- OEM
- Corporate (B2B companies)

3.3 Sponsorship and/or affiliation

CSIRT-HORNETSECURITY is affiliated to the Hornetsecurity company (https://www.hornetsecurity.com).

3.4 Authority

CSIRT-HORNETSECURITY operates under the authority of Hornetsecurity Head of TIRC and CISO.

4 Policies

4.1 Types of incidents and level of support

CSIRT-HORNETSECURITY handles all malicious emails occurring in Hornetsecurity’s constituents’ mailboxes.
The level of support provided by CSIRT-HORNETSECURITY will be contingent upon the severity of the security incident or issue, its assessed impact, and the resources available to CSIRT-HORNETSECURITY at the time of the incident.

4.2 Co-operation, interaction and disclosure of information

CSIRT-HORNETSECURITY 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-HORNETSECURITY’s efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when CSIRT-HORNETSECURITY’s cooperation is likely to enable third-party CERTs, CSIRTS and other security teams to better perform their duties and resolve incidents.
CSIRT-HORNETSECURITY operates within the current French legal framework.

4.3 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.

5 Services

5.1 Announcements

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

5.2 Indicators of compromised publication

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

5.3 Education and training

CSIRT-HORNETSECURITY 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.

5.4 Analyse malicious email campaign

CSIRT-HORNETSECURITY 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-HORNETSECURITY's threat intelligence.
- In response, CSIRT-HORNETSECURITY examines how Hornetsecurity 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-HORNETSECURITY closely monitors the evolving threat landscape. This allows for the ongoing adaptation of measures and protections to safeguard the interests of its constituents.

6 Incident reporting

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

- 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-HORNETSECURITY, please include all relevant email headers, bodies and attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

7 Disclaimer

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