CERT Hermès

RFC 2350

CONTENTS

1. DIFFUSION

TLP:WHITE

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:WHITE information may be distributed without restriction, subject to copyright controls.

2. DOCUMENT INFORMATION

This document contains a description of CERT Hermès as implemented by RFC 2350.

It provides basic information about CERT Hermès, its channels of communication, its roles and responsibilities.

RFC 2350 is an IETF Best Current Practice available at: https://www.ietf.org/rfc/rfc2350.txt

2.1. DATE OF LAST UPDATE

15/04/2022 - version 1.0

2.2. DISTRIBUTION LIST

There is no distribution list for notifications.

2.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this this CERT description may be found at:
https://www.hermes.com/cert/rfc2350.pdf

2.4. AUTHENTICATING THIS DOCUMENT

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

The signature of this document is available at: https://www.hermes.com/cert/rfc2350.pdf.sig

2.5. DOCUMENT IDENTIFICATION

Title	CERT Hermès - RFC2350
Version	1.0
Document Date	06 April 2022
Expiration	This document is valid until superseded by a later version

3. CONTACT INFORMATION

3.1. NAME OF THE TEAM

CERT Hermès

3.2. ADDRESS

CERT Hermès – Campus Cyber

5-7 Rue Bellini

92800 Puteaux

FRANCE

3.3. TIMEZONE

- **CET** (From October to March, UTC+1)
- **CEST** (From March to October, UTC+2)

3.4. TELEPHONE NUMBER

No Phone number available

3.5. FACSIMILE NUMBER

None available

3.6. OTHER MEANS FOR COMMUNICATION

None

3.7. ELECTRONIC MAIL ADDRESS

cert(at)hermes(dot)com

This is a mail alias that relays mail to the human(s) on duty for the CERT Hermès.

3.8. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

CERT Hermès has a PGP public Key available at https://keys.openpgp.org/ :

Key ID is "6ABF 5B9B EAAB 2F66"

The key is also published and available at : https://www.hermes.com/cert/cert_hermes_public.asc

3.9. TEAM MEMBER

Raphael ELLOUZ is the current CERT Hermès team leader. The team consists of IT security analysts.

This list is not publicly available.

3.10. OTHER INFORMATION

None available

3.11. POINTS OF CONTACT

The preferred method to contact CERT Hermès is to send e-mail to the cert (at)hermes(dot)com address.

"This mailbox is actively monitored to answer in a proper manner."

4. CHARTER

4.1. MISSION STATEMENT

CERT stands for "Computer Emergency Response Team".

CERT Hermès mission is to coordinate and investigate IT security incident response for global Hermès Group.

CERT Hermès will investigate any security incident that may involve the Hermès group or any Hermès entity as a source or target of an attack or any cyber-threat.

- Provide a 360 view and in-depth analysis of the past incidents. Preventive protocols could be set up in the light of these reports that Cert provide after the incidents.
- Informing related departments about new technologies, policies and changes in protocols after security incidents.
- Ensure that the security response team skills stay sharp by providing continuous cybersecurity training.
- Creating and (when necessary) updating the incident response plan (IRP).
- Preserving confidentiality during incidents.
- Regularly reviewing standard security protocols and if needed, updating them.
- Contribute to the practical application of the ISSP defined by the governance.
- At the same time, CERT Hermès is carrying out security monitoring (new attacks, new malware, the latest vulnerabilities) to "know" the state of the threat and assess its own vulnerabilities. An active scanning on exposed assets is done periodically for this purpose.
- CERT Hermès is responsible for identifying new critical vulnerabilities targeting and ensuring that remediation actions have been taken to cover the risk.
- CERT Hermès team can also be called upon by other teams to provide its expertise as a consultant/advisor on various projects for other Hermès teams. These teams are not necessarily in IT.

4.2. CONSTITUENCY

Our constituency are composed of Hermès Group and all the entities within the Group.

The full list of the entities within Hermès Group is not disclosed here.

4.3. SPONSORSHIP AND/OR AFFILIATION

CERT Hermès is the Computer Security Incident Response Team for the Hermès Group

Funding is provided by the Hermès group.

4.4. AUTHORITY

CERT Hermès operates under the authority of the management of the Hermès Group.

5. POLICIES

5.1. TYPE OF INCIDENTS AND LEVEL OF SUPPORT

CERT Hermès addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident, the number of affected entities within our constituency, and our resources at the time.

Usually, our first response comes on the same working day during working hours, if not it will be on the following working day.

5.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT Hermès will exchange all necessary information with other CSIRTs as well as with other affected parties if they are involved in the incident or incident response process.

No incident or vulnerability related information will be given to other persons.

Our first priorities are to preserve:

- The level of confidentiality assigned to information by its owner. We use "TLP" protocol (as define by FIRST: https://www.first.org/tlp/) to define information confidentiality.

- The privacy of personal information. No sensitive information will be sent by CERT Hermès to another party without a prior agreement of the information owner.

- French law enforcement personnel requesting information during a criminal investigation will be given the requested information within the limits of the court order and the criminal investigation if they present a valid court order from a French court.

5.3. COMMUNICATION AND AUTHENTICATION

All e-mails sent to the Hermès Group should be signed using PGP.

All e-mails containing confidential information should be encrypted and signed using PGP. Information received in encrypted form should not be stored permanently in unencrypted form. For other communication, a phone call, postal service, or unencrypted e-mail may be used.

CERT Hermès supports the Information Sharing Traffic Light Protocol (TLP)

6. SERVICES

6.1. ANNOUNCEMENTS

CERT Hermès provides announcements in the form of alerts and security briefings featuring threat intelligence of different sorts, which may include, but is not limited to detected vulnerabilities, new attack tools, techniques and processes as leveraged by the threat actors, indicators of compromise, and security measures needed to protect the Information Systems of Hermès Group.

6.2 ALERTS AND WARNINGS

CERT Hermès disseminates information and intelligence on cyberattacks, technical disruptions, security vulnerabilities, intrusions, malware, and provides recommendations on how to tackle the resulting risk within its constituency.

Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis.

6.2. INCIDENT RESPONSE

CERT Hermès will assist system administrators 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:

6.2.1. INCIDENT TRIAGE

- Interpretation of incoming security alerts, prioritization and relating them to ongoing incidents and trends.
- Investigating whether indeed an incident occurred and its scope.

6.2.2. INCIDENT COORDINATION

Incident Coordination includes:

- **Information Categorization:**

CERT Hermès maintains a mapped list between the machines and the machines involved in the incident with respect to the information disclosure policy

- **Coordination:**

CERT Hermès analysts notify involved parties on a need-to-know basis, as per the information disclosure policy.

6.2.3. INCIDENT RESOLUTION

- **Technical Assistance**

CERT Hermès analysts offer digital investigation support

- **Eradication**

CERT Hermès analysts can propose solutions or take actions to eradicate the threat on the affected computers or follow up on the resolution of the exploited vulnerability.

- **Recovery**

CERT Hermès analysts can propose solutions to restore affected systems and services to their status before the security incident.

6.3. PROACTIVE

The team offers the following services:

6.3.1. INTRUSION DETECTION SERVICES

CERT Hermès leverages tools, services and processes to detect potential intrusions.

6.3.2. AUDITING SERVICES

- **Information provision**

CERT Hermès maintains an history of all past security incidents / critical vulnerabilities it dealt with.

- **Education and training**

CERT Hermès analysts are offered training according to the needs of the team and the skills of each individual.

- **Site security auditing and consulting**

- **Product evaluation**

6.4. OTHER SERVICES

Hermès has also a "vulnerability disclosure policy" (VDP).

Please see : https://vdp.hermes.com for more information.

7. INCIDENT REPORTING FORMS

CERT Hermès does not have an incident reporting form.

Please report security incidents via encrypted email to cert(at)Hermes(dot)com

Incident reports should contain the following information:

- Incident date and time (including time zone)
- Source IPs, ports, and protocols
- Destination IPs, ports, and protocols
- And any relevant information

8. DISCLAIMER

This document is provided 'as is' without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. If you notice any mistakes within this document, please send a message to us by e-mail.

We will try to resolve such issues as soon as possible.