L3 LIMITED

RFC 2350

TEHTRIS-CERT

1. Document Information

1.1 Date of Last Update

This is version 2, published 2022/11/15.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

The current version of this this CERT description may be found at https://tehtris.com/en/services/cert/ and https://tehtris.com/fr/services/cert-csirt/

1.4 Authenticating this Document

This document has been signed with the PGP key of CERT TEHTRIS. The signature of this document is available at https://tehtris.com/en/services/cert/

1.5 Document Identification

Title : TEHTRIS-CERT – RFC 2350
Version: 2.0
Document Date: 2022/11/15
Expiration: this document is valid until superseded by a later version

2. Contact Information

2.1 Name of the Team

TEHTRIS-CERT

2.2 Address

TEHTRIS-CERT
5 allée des Lumières
Cité de la Photonique
33600 PESSAC FRANCE

2.3 Time Zone

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

2.4 Telephone Number

Phone: +33 (0) 9-72-43-07-64

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication

Not available.

2.7 Electronic Mail Address

cert@tehtris.com
This is a mail alias that relays mail to the human(s) on duty for TEHTRIS-CERT.

2.8 Public Keys and Encryption Information

CERT TEHTRIS is using the following PGP key for its email exchanges with cert (at) tehtris (dot) com address:
ID: 749D 7D58 DFB4 2A70
Fingerprint: 3750 DAA0 F867 4B2B 1FBC 0385 749D 7D58 DFB4 2A70

2.9 Team Members

The list of the TEHTRIS-CERT's team members is not publicly available. The team consists of Cybersecurity Analysts.

2.10 Other Information

None.

2.11 Points of Customer Contact

The preferred method to contact TEHTRIS-CERT is by sending an email to the following address: cert@tehtris.com. A security analyst can be contacted at this email address during hours of operation.

Urgent cases can be reported by phone (+33 (0) 9-72-43-07-64) during 8.30 am and 5.30 pm (UTC+2).

3. Charter

3.1 Mission Statement

TEHTRIS-CERT's core mission is to provide information, guidance, and assistance to reduce the risks of information security incidents as well as to lead the response to such incidents in a timely manner when/if they occur.

In addition to incident response, TEHTRIS-CERT proactively gathers, analyzes, and communicates on relevant threat intelligence in order to identify and protect from emerging cybercriminal trends and contribute to global cybersecurity.

3.2 Constituency

TEHTRIS-CERT's constituency consists of TEHTRIS infrastructure and its user base.

3.3 Sponsorship and/or Affiliation

TEHTRIS-CERT is part of TEHTRIS and maintains relationships with various CERT/CSIRT teams throughout the world.

3.4 Authority

TEHTRIS-CERT operates under the authority of TEHTRIS CTO, Laurent OUDOT.

4. Policies

4.1 Types of Incidents and Level of Support

TEHTRIS-CERT manages all type of cybersecurity incidents that occur, or threaten to occur, within its constituency.

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

4.2 Co-operation, Interaction and Disclosure of Information

TEHTRIS-CERT operates under the restrictions imposed by French and European laws and accordingly to GDPR.

TEHTRIS-CERT exchanges all necessary non-restricted information with other CSIRTs / CERTs as well as with other affected parties involved in the incident or incident response process.

TEHTRIS-CERT members take part in extended CSIRT networks as well as cybersecurity organizations in order to contribute to the exchange of cybersecurity knowledge.

4.3 Communication and Authentication

TEHTRIS-CERT recommends sending all information through encrypted email (through OpenPGP).
TEHTRIS-CERT supports the TLP (Traffic Light Protocol) in order to classify information.

5. Services

TEHTRIS-CERT offers the following services to its constituency:

- Threat Intelligence
- Incident response on TEHTRIS' infrastructure

5.1 Incident Response

TEHTRIS-CERT, supported by other TEHTRIS cybersecurity teams, provides the following services:

- Incident triage: assessment of the severity of the incident and attribution of a criticality score
- Incident coordination: implementation of a response plan by dividing up tasks and tracking progress, collecting technical evidence to determine the initial cause of the incident and investigating on collateral damage
- Incident resolution: proposition of corrective measures, communication to the team concerned by the incident, publication of a forensic report

5.2 Proactive Activities

In order to raise awareness among collaborators and to prevent incidents from happening, TEHTRIS-CERT offers the following proactive activities services:

- Threat Hunting
- Technology watch

- Cyber Threat Intelligence
- Cyber security alerts publication

6. Incident Reporting Forms

TEHTRIS-CERT does not have public incident reporting form.

7. Disclaimers

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

Eléna POINCET

Signed by Eléna POINCET
Signé et certifié par yousign

Laurent Oudot

Signed by Laurent Oudot
Signé et certifié par yousign