RFC 2350
CSIRT-TEHTRIS
[CERT-TEHTRIS]

1 Document information 2
1.1 Date of Last Update 2
1.2 Distribution List for Notifications 2
1.3 Locations where this Document May Be Found 2
1.4 Authenticating this Document 2
2 Contact Information 3
2.1 Name of the Team 3
2.2 Address 3
2.3 Timezone 3
2.4 Telephone Number 3
2.5 Facsimile Number 3
2.6 Other Telecommunication 3
2.7 Electronic Mail Address 3
2.8 Public Keys and Other Encryption Information 4
2.9 Team Members 4
2.10 Other Information 4
2.11 Points of Customer Contact 4
3 Charter 5
3.1 Mission Statement 5
3.2 Constituency 5
3.3 Sponsorship and/or Affiliation 5
3.4 Authority 5
4 Policies 6
4.1 Type of Incidents and Level of Support 6
4.2 Co-operation, Interaction and Disclosure of Information 6
4.3 Communication and Authentication 6
5 Services 7
5.1 Pre-emptive Security Measures 7
5.2 Incident Response 7
5.3 Proactive Activities 8
6 Incident Reporting Forms 9

1 Document information

This document contains a description of CSIRT TEHTRIS eGambit (CSIRT-TEHTRIS) as implemented by RFC 2350. It provides basic information about CSIRT-TEHTRIS, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

Version 1.2 2016/11/30 update 2016
Version 1.1 2015/11/30 update 2015
Version 1.0 2015/06/24 initial

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 CSIRT description may always be found at http://www.tehtris.com/csirt

1.4 Authenticating this Document

This document has been signed with the PGP key of CSIRT-TEHTRIS. The signature of this document is available at http://www.tehtris.com/csirt

2 Contact Information

2.1 Name of the Team

Short name: “CSIRT-TEHTRIS”
Long name: “CSIRT TEHTRI-Security eGambit”

CERT name: “CERT-TEHTRIS”

2.2 Address

TEHTRI-Security
CSIRT-TEHTRIS
13-15 rue Taitbout
75009, PARIS
FRANCE

2.3 Timezone

CET/CEST

2.4 Telephone Number

Phone: +33 (0) 9-72-50-80-33 [inputs are filtered, but all messages are monitored]

2.5 Facsimile Number

Fax: +33 (0) 1-72-71-25-99

2.6 Other means for communication

Twitter: @tehtris

2.7 Electronic Mail Address

cert (at) tehtris (dot) com
This is a mail alias that relays mail to the human(s) on duty for the CSIRT-TEHTRIS

2.8 Public Keys and Other Encryption Information

CSIRT-TEHTRIS is using the following PGP key for its email exchanges with cert (at) tehtris (dot) com address:

- ID: 8F281158
- Fingerprint: 1416 56B6 2D67 55E9 2018 5BA7 BDE8 A13A 8F28 1158

2.9 Team Members

Laurent Oudot (CEO at TEHTRIS) is the direct CSIRT-TEHTRIS team leader.

The other members of the CSIRT team are the TEHTRIS security experts and consultants.

2.10 Other Information

None

2.11 Points of Customer Contact

The preferred method to contact CSIRT-TEHTRIS is to send e-mail to the cert (at) tehtris (dot) com address.

This mailbox is monitored actively during hours of operations.

Standard hours of operations:
7h00 - 22h00 from Monday to Friday
8h00 - 20h00 on Weekends

The mailbox is monitored 365 days / 365.

3 Charter

3.1 Mission Statement

The purpose of the CSIRT is, first, to assist its customer community in implementing proactive measures to reduce the risks of computer security incidents, and second, to assist its customer community in responding to such incidents when they occur.

3.2 Constituency

CSIRT-TEHTRIS constituency is composed of all the customer of the TEHTRIS eGambit solution who subscribed a Service Level Agreement support contract.

3.3 Sponsorship and/or Affiliation

CSIRT-TEHTRIS is part of TEHTRIS.
CSIRT-TEHTRIS maintains relationships with various CSIRTs throughout the world, on all continents, on an as-needed basis.

3.4 Authority

As CSIRT-TEHTRIS is aimed to handle incident response on customers' perimeter, CSIRT-TEHTRIS has an advisor role with local security teams and has no specific authority to require any specific action. The recommendations, which CSIRT-TEHTRIS will provide to a customer, will be implemented under the direction of the concerned customer.

4 Policies

4.1 Type of Incidents and Level of Support

CSIRT-TEHTRIS is generally mandated by its customer to handle any type of incident occurring on its own perimeter.
Depending on the type of security incident, CSIRT-TEHTRIS will gradually roll out its services, which include incident response and digital forensics.

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT-TEHTRIS operates under the restrictions imposed by French laws.

All information exchanged with a customer during an incident (and after its resolution) will be handled confidentially in secure environments using encryption if necessary.

CSIRT-TEHTRIS will cooperate with other Organizations in the Field of Computer Security, which may help to deliver its services, especially for incident resolution. In any such exchange, CSIRT-TEHTRIS will protect the privacy of its customers through anonymisation of technical data that may be exchanged. Customers will be informed of such exchanges.

If a customer objects the default CSIRT-TEHTRIS behavior, it should be specified in initial contractual agreement or explicitly asked in the communication with CSIRT-TEHTRIS. Requiring specific behavior may lower the quality of assistance CSIRT-TEHTRIS may provide.

4.3 Communication and Authentication

For normal communication without any sensitive information, unencrypted e-mail may be used use but CSIRT-TEHTRIS strongly encourage customer to use encrypted email (through PGP) to exchange data with CSIRT-TEHTRIS.

5 Services

5.1 Pre-emptive Security Measures

As the CSIRT-TEHTRIS services are delivered to TEHTRIS eGambit customer, CSIRT-TEHTRIS will implement in eGambit tool, or provide information to eGambit developers, any technical security measure that may help to detect or block security threats, including emerging ones.

5.2 Incident Response

CSIRT-TEHTRIS is mandated, by its customer, to be responsible for the coordination of security incidents somehow involving customers' perimeters. The technical resolution of incident if operationally left to local customers administrators with CSIRT-TEHTRIS support.

Without being exhaustive, following aspects are covered by CSIRT-TEHTRIS:

- 5.1.1 Incident Triage
  - Investigating whether indeed an incident occurred
  - Determining the extent of the incident.

- 5.1.2 Incident Coordination
  - Determining the initial cause of the incident (vulnerability exploited).
  - Facilitating contact with other sites, that may be involved.
  - Facilitating contact with appropriate law enforcement officials, if necessary.
  - Making reports to other CSIRTs.
  - Composing announcements to users, if applicable.

- 5.1.3 Incident Resolution
  - Providing action plan to remove the vulnerability and supporting local administrators to perform the action plan.
  - Providing action plan and support to help securing the system from the effects of the incident.
  - Evaluating whether certain actions are likely to reap results in proportion to their cost and risk
  - Providing action plan and support to collect any evidence after the fact in order to be used in criminal prosecution or any disciplinary action

5.3 Proactive Activities

CSIRT-TEHTRIS performs the following proactive activities:

- Technology watch
- Intrusion detection
- Development of security tools
- Information about major security threats or vulnerabilities to its customers
- Training on security topics

6 Incident Reporting Forms

No public form is proposed on our web site, to report incidents to CSIRT-TEHTRIS, but you can directly use the email contact with proper information when needed. eGambit subscribers can use internal tools in eGambit frontend to share events and needed information"

In case of emergency or crisis, please provide to CSIRT-TEHTRIS 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) and/or any extract from the log showing the problem;