TE RAMA

CSIRT-TERAMA

RFC-2350

VERSION 1.0 DU 29/01/2024

TLP:CLEAR

1 Document Information

This document follows the RFC2350 specification (https://www.ietf.org/rfc/rfc2350.txt) 1.1.

1.1 Date of last update

Version 1.0, published the 30th January 2023

1.2 Distribution list for notifications

There is no distribution list for notifications. The current version of this document may be found at

Location where this document may be found https://github.com/CSIRT-TERAMA/ressources

1.3 Authenticating this document

This document has been signed with the CSIRT-TERAMA PGP key. See section 2.8 for more details.

2 Contact Information

2.1 Name of the Team

CSIRT-TERAMA

2.2 Address

CSIRT-TERAMA offices are located in French Polynesia:

Te Rama,

32 rue Tepano Jaussen,

PAPEETE, Polynésie française

2.3 Time Zone

Tahiti Time (TAHT) (UTC-10)

2.4 Telephone Number

Office number (French Polynesia prefix): +(689) 40 455 200

2.5 Facsimile Number

N/A

2.6 Other Telecommunication

N/A

2.7 Electronic Mail Address

Communication from other CSIRT or if you experienced an incident and need support :

cisrt @terama.pf

2.8 Public Keys and Encryption Information

- Fingerprint : 287E CCC6 3E31 93EF EE15 0CFE 70CD 0ABD BCFF EC3C
- Key ID : 0x70CD0ABDBCFFEC3C
- Expire : 30/01/2027
- User ID : CSIRT-TERAMA
- https://github.com/CSIRT-TERAMA/ressources/blob/main/CSIRT-TERAMA_0xBCFFEC3C_public.asc

2.9 Team Members

• Jérémy MOUNIER : team leader of the Incident Response Team

• Team members not publicly available

2.10 Other Information

https://www.terama.pf/ for other information.

2.11 Points of Customer

Contact CSIRT-TERAMA is the operational point of contact only during business hours. Out of business hours requests are processed only for registered clients. For any commercial purpose, contact @ terama.pf

3 CHARTER

3.1 Mission Statement

CSIRT-TERAMA's first goal is providing support on cybersecurity incident anticipation and response to TERAMA's group, to our new and existing customers.

We are committed to capitalize technical and non-technical information in order to give a continuous understanding of threat actors and cyber operations targeting first French-Polynesia and widely pacific area.

Our incident response team will provide assistance to understand and investigate incidents and help to mitigate the attack.

CSIRT-TERAMA is a consulting company not affiliated or linked with a dedicated commercial vendor.

3.2 Constituency

Any customer with an IT-related incident can ask CSIRT-TERAMA for an incident response service as described on the website www.terama.pf/. Public or Private sector.

3.3 Sponsorship and/or Affiliation

CSIRT-TERAMA is part of TERAMA a French Polynesian company. It maintains relationships with various CSIRTs throughout the world, on all continents, on an as-needed basis and with the French national CERT-FR

3.4 Authority

As CSIRT-TERAMA is aimed to handle incident responses on customers' perimeter, CSIRT-TERAMA has an advisory role with local IT/ Security teams and has no specific authority to require any specific action. Any recommendation which CSIRT-TERAMA may provide will be implemented under the direction of the customer.

4 POLICIES

4.1 Types of Incidents and Level of Support

CSIRT-TERAMA is generally mandated by its customers to handle any type of incident occurring within their own perimeter. Depending on the type of security incident, CSIRT-TERAMA will gradually roll out its services, which include incident response and digital forensics. CSIRT-TERAMA services include preventive, reactive and proactive services:

- Alerts and warnings ;
- Incident analysis and forensics ;
- Incident response assistance and support ;
- Incident response and remediation ;
- Incident and crisis management services
- Threat intelligence analysis and sharing.
- Cybersecurity awareness and training

In addition, CSIRT-TERAMA liaises and can rely on the expertise and knowledge provided by other TERAMA services.

5 SERVICES

Incident Management services:

- Incident response methodologies
- Digital forensics and investigation support
- Incident response and crisis support
- Remediation support
- Incident and crisis training exercises

Vulnerability Management services:

- Vulnerability watch and alerts
- Domain monitoring
- Public infrastructure monitoring
- Data leak monitoring
- Threat hunting

6 INCIDENT REPORTING FORMS

No public form is proposed on our web site to report incident to CSIRT-TERAMA, but you can directly use the dedicated email address (using the PGP Key) : csirt @ terama.pf with proper information when needed :

- What : the scope and type of suspected or compromised systems , IP address(es), FQDN(s), and any other relevant technical element with the associated observations
- When : A timeline of key known elements

- Who : Contact details and organizational information (minimal): name of the person, organization name, email address and telephone number, the name of people affected by the incident
- Where : the physical location of the affected systems or the cloud provider (region) A phone call is usually followed up to complete and fill out the understanding of the incident

7 DISCLAMERS

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