

| | | | |
|--|---|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | TLP:CLEAR Information may be distributed without restriction. Subject to copyright controls. | Page | [1] |



RFC 2350 DJ-CERT

Version 1.0 - 2023-11-30

| | | | |
|---|---|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | <p style="text-align: center;">TLP:CLEAR</p> Information may be distributed without restriction. Subject to copyright controls. | Page | [2] |

1. Document Information

This document contains a description of DJ-CERT in accordance with RFC 2350 specification. It provides basic information about DJ-CERT, describes its responsibilities and services offered.

1.1. Date of Last Update

Version 1.0, published on 2023-11-30.

1.2. Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism to inform of changes made to this document.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available at DJ-CERT's website at: https://cert.gouv.dj/uploads/contact/DJ-CERT_RFC2350_EN.pdf

1.4. Authenticating this Document

This document has been signed with the PGP key of DJ-CERT. The signature and our public PGP key are available on our website: <https://cert.gouv.dj/contact>

DJ-CERT's public PGP key is given at chapter 2.8 below.


1.5. Document Identification

Title: 'DJ-CERT_RFC2350_EN'

Version: 1.0

Document Date: 2022-11-30

Expiration: this document is valid until superseded by a later version

| | | | |
|---|---------------------------------------|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | TLP:CLEAR | Page | [3] |
| Information may be distributed without restriction. Subject to copyright controls. | | | |

2. Contact Information

2.1. Name of the Team

Official name:

Centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques (Djiboutian government Computer emergency response team).

Short name:

DJ-CERT

2.2. Address

Présidence De La République
SGG/ANSIE/DJ-CERT

Avenue Adm. Bemard, Djibouti

2.3. Time Zone

GMT +03

2.4. Telephone Number

Main number (duty office): +253 21-44-11-12

2.5. Facsimile Number

Not applicable

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Address


If you need to notify us about an information security incident or a cyber-threat targeting or involving DJ-CERT, please contact us at: incident@cert.gouv.dj

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with DJ-CERT.

- User ID: DJ-CERT(Djiboutian Computer Emergency Response Team)
contact@cert.gouv.dj
- Fingerprint: 4B84D33A5EE332DBD4EBDD882827C46E0CF88A41

The public PGP key is available at the following location:
https://cert.gouv.dj/uploads/contact/DJ-CERT_public.asc

| | | | |
|---|---|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | <p style="text-align: center;">TLP:CLEAR</p> Information may be distributed without restriction. Subject to copyright controls. | Page | [4] |

2.9. Team Members

DJ-CERT team is composed of IT security experts. The list of DJ-CERT team's members is not publicly available.

2.10. Other Information

See our web site at <https://cert.gouv.dj/> for additional information about DJ-CERT.

2.11. Points of Customer Contact

DJ-CERT prefers to receive incident reports via e-mail at incident@cert.gouv.dj. Please use our cryptographic key to ensure integrity and confidentiality.

3. Charter

3.1. Mission Statement

DJ-CERT is the Computer Emergency Response Team (CERT) of the Djiboutian National agency of the state information system. Its mission is to strengthen the capacities of the Republic of Djibouti to combat cyber-attacks by ensuring coordination and sharing of information relating to new threats and incidents

DJ-CERT's missions cover prevention, detection, response and recovery.

3.2. Constituency

- All ministries, administrations and state services;
- Critical national infrastructure operators and operators of essential services.

In order to have more information, please take a look at the DJ-CERT website <https://cert.gouv.dj>

3.3. Affiliation

DJ-CERT is part of ANSIE (Agence Nationale des Systèmes d'Information de l'Etat), the Djiboutian National Information System.

It has a communication channel with CSIRT.tn

3.4. Authority

Presidency of the Republic of Djibouti
SGG –General Secretariat of Government
ANSIE/DJ-CERT operates under the SGG

| | | | |
|---|---|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | <p style="text-align: center;">TLP:CLEAR</p> Information may be distributed without restriction. Subject to copyright controls. | Page | [5] |

4. Policies

4.1. Types of Incidents and Level of Support

DJ-CERT is the central point of contact regarding security-related computer incidents in Djibouti. DJ-CERT's support levels are contingent on several factors, including the nature and severity of the incident, the type of affected party, the significance of the impact on critical infrastructure or services.

The main services offered now by DJ-CERT are:

- Alerts and warnings;
- Cyber threat Intelligence;
- Incident response Coordination & collaboration.

4.2. Co-operation, Interaction and Disclosure of Information

To accomplish its mission and perform its services, DJ-CERT regularly interacts with other organisations, such as other CERT or CSIRT teams, Vendors, vulnerability Reporters, etc.

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

4.3. Communication and Authentication

The preferred method of communication is email. For low sensitivity information, unencrypted methods such as email or telephones can be used.

All sensitive communication to DJ-CERT should be encrypted with our public PGP key as detailed in Section 2.8.

| | | | |
|---|---|------|------------|
|  | DJ-CERT description – RFC 2350 | Date | 2023-11-30 |
| | <p style="text-align: center;">TLP:CLEAR</p> Information may be distributed without restriction. Subject to copyright controls. | Page | [6] |

5. Services

5.1. Incident response

DJ-CERT's incident response services are available on business hours: Sunday to Thursday, 8:00AM to 5:00PM.

5.2. Incident Triage

- Assessment of the severity of the incident & prioritation

5.3. Incident Coordination

- Categorization of the incident-related information with respect to the information disclosure policy;
- Facilitate coordination between different constituencies to harmonize incident response efforts.

5.4. Incident Resolution

- Analysis of compromised systems;
- Elimination of the cause of a security incident
- Restore affected systems and services to their state before the security incident

5.5. Proactive activities

- Warning and information services available at <https://cert.gouv.dj> ;
- Network monitoring to detect attacks as early as possible;

6. Incident Reporting Forms

To report an incident to DJ-CERT, please visit <https://cert.gouv.dj/Declaration/>

7. Disclaimers

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