DATTAK.

RFC 2350

CERT-DATTAK

1. Document information

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

1.1. Date of last update

Version 1.1, published on 13/08/2025.

1.2. Distribution list for notification

There is no distribution list for notifications. Therefore, changes will not be actively notified. Please send questions about updates to the CERT-DATTAK team email address : cert@dattak.io.

1.3. Locations where this document can be found

The current and latest version of this document is available at CERT-DATTAK's website at:https://www.dattak.io/fr/cert

1.4. Authenticating this document

This document has been signed with the GPG key of CERT-DATTAK. The signature and our public GPG key (ID and fingerprint) are available on our website: https://www.dattak.io/fr/cert

1.5. Document Identification

Title: 'CERT-DATTAK_RFC2350_EN'
Version: 1.1
Document Date: 13/08/2025.
Expiration: this document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

CERT-DATTAK is DATTAK's commercial emergency response team.

2.2. Address

CERT-DATTAK
21 RUE DU GÉNÉRAL FOY
75008 PARIS, FRANCE

2.3. Time Zone

CET/CEST

2.4. Telephone number

+33 1 76 41 12 75

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 CERT-DATTAK, please contact us at: cert@dattak.io

2.8. Public keys and encryption information

GPG is used for functional exchanges with CERT-DATTAK.

- User ID: CERT-DATTAK <cert@dattak.io>
- Key ID: 0xBA8868BA8BB0C047
- Key Type :
    - Ed25519 for signing (ID : DF8F5BC65F8B6B14)
    - Curve25519 for encryption (ID : 02E113E6AD984D1B)
- Fingerprint: F8C4EDE211B2B687E34B3DC3BA8868BA8BB0C047

The public GPG key is available at the following location:
https://www.dattak.io/fr/cert

Please use this key to:

- Encrypt any confidential information sent to our team.
- Verify any signed messages from our team.

2.9. Team members

The CERT-DATTAK team is composed of IT security experts. The list of CERT-DATTAK team members is not publicly available. The identity of CERT-DATTAK team's members might be divulged on a case-by-case basis according to the need-to-know restrictions.

2.10. Other information

Additional information about CERT-DATTAK can be found at https://www.dattak.io/fr/cert/

2.11. Points of customer contact

CERT-DATTAK prefers to receive incident reports via e-mail at cert@dattak.io. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please use the [URGENT] tag in the subject field in your e-mail.

CERT-DATTAK's hours of operation are 24/7.

3. Charter

3.1. Mission statement

CERT-DATTAK is DATTAK's Computer Emergency Response Team (CERT). Our mission is to coordinate and investigate IT security incidents affecting DATTAK's customers. To fulfill this mission, CERT-DATTAK focuses on the following points:

- Proactively preventing security incidents through advisory services, awareness training, and configuration reviews.
- Effectively managing incident response efforts, collaborating with trusted partners as needed.

3.2. Constituency

CERT-DATTAK provides services to its Customers Community, who subscribed support contracts.

3.3. Affiliation

CERT-DATTAK is part of DATTAK.
CERT-DATTAK maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis.

3.4. Authority

CERT-DATTAK operates within the framework of contracts, validated and signed with its customers.
The team has no authority to request the performance of actions on the systems and networks on the impacted perimeters.

4. Policies

4.1. Types of incidents and level of support

CERT-DATTAK provides an initial diagnosis and coordinates any IT security incident that targets or could target its scope of action (3.2). Depending on the nature of the incident, CERT-DATTAK informs the parties capable of remedying it.
The level of service offered by CERT-DATTAK varies according to the type of incident, its criticality, and the resources available to deal with it.
CERT-DATTAK's services include reactive and proactive services:

- 24/7 on-call duty;
- Incident analysis and forensics;
- Incident response assistance and support;
- Incident response and remediation ;
- Vulnerability and malware analysis;
- Vulnerability response;

4.2. Co-operation, interaction and disclosure of information

Incident-related information, such as names and technical details, is not published without the express consent of all relevant stakeholders. If not agreed otherwise, supplied information is kept confidential. CERT-DATTAK will never pass information to third parties unless required by law. Under the condition of acceptance through affected parties or authorized by law, CERT-DATTAK prefers to share Tactics,

Techniques and Procedures for the purpose of prevention and reaction to specific incidents.

Our first priorities are to preserve:

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

No sensitive information will be sent by CERT-DATTAK to another party without a prior agreement of the information owner. CERT-DATTAK handles and processes information in secured physical and technical environments in accordance with the French state regulations for the protection of information.

4.3. Communication and authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CERT-DATTAK uses GPGfor encrypting and/or signing messages. All sensitive communication to CERT-DATTAK should be encrypted with our public GPG key as detailed in Section 2.8.

5. Services

5.1. Incident response

CERT-DATTAK's incident response services are available on a 24/7 basis to our constituency. All information and communication technologies related incidents are evaluated. Indepth analysis is provided by technical experts.

5.2. Incident triage

CERT-DATTAK's incident triage process involves several key steps to assess and prioritize reported incidents:

- Collection of information about the incident.
- Confirmation that the described event is actually a cyber security incident and is related to our constituency.
- Assessment of the severity of the incident (what is the impact) and its extent (how many computers are affected).

5.3. Incident coordination

- Categorization of the incident-related information (log files, contact information, etc.) with respect to the information disclosure policy;

- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.4. Incident resolution

- Analysis of compromised systems;
- Elimination of the cause of a security incident (exploited vulnerability), and its effects.

5.5. Proactive activities

Other services proposed by CERT-DATTAK to its customers as proactive activities regarding cybersecurity include:

- **Vulnerability scanning**: Regular scanning of publicly available systems to identify known vulnerabilities. This allows for proactive patching and mitigation of risks.
- **Scan AD**: Assessment of Active Directory configuration. This service identifies potential misconfigurations and vulnerabilities within the Active Directory environment.
- **Scan Cloud**: Assessment of Cloud configuration. This service analyzes the customer's cloud environment to detect security weaknesses and compliance issues.
- **Penetration testing**: Simulated cyberattacks to identify exploitable vulnerabilities in systems and applications. This helps to assess the effectiveness of existing security controls.
- **Cybersecurity training**: Providing training sessions and workshops to raise awareness about cybersecurity best practices and potential threats. This helps to empower the customer's staff and improve their overall security posture.

These proactive activities help our customers to identify and mitigate security risks before they can be exploited by attackers, strengthening their overall cybersecurity posture.

6. Incident reporting Forms

No local form has been developed to report incidents to CERT-DATTAK. If possible, please provide the following information :

- Contact information, including electronic mail address and telephone number
- Date and time when the incident started
- Date and time when the incident was detected
- Incident description
- Affected assets, impact

- Actions taken so far

7. Disclaimer

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