RFC 2350 — CERT Harmattan AI

TLP:CLEAR

This document describes the Computer Emergency Response Team (CERT) Harmattan AI in accordance with **RFC 2350**, *Expectations for Computer Security Incident Response*. It provides basic information about the team, the ways it can be contacted, its responsibilities, and the services it offers.

www.harmattan.ai
1 Rue du Mail, 75002 Paris FRANCE

Content

1. Document Information

1.1 Date of Last Update

This is version 1.0, published [2026-08-27].

1.2 Distribution List for Notifications

There is no formal distribution list for notifications of changes to this document. Questions about updates may be directed to the CERT at the email address given in Section 2.7. Constituents who wish to be notified of changes may request inclusion on an internal announcement list by contacting the team.

1.3 Locations where this Document May Be Found

The current version of this document is available at:

https://www.harmattan.ai/cert/rfc2350.pdf

The version at this location is authoritative. Whenever the document is updated, the date in Section 1.1 will change accordingly.

1.4 Authenticating this Document

This document has been signed with the PGP/GnuPG key of the CERT Harmattan AI. The detached signature is available alongside the document at:

https://www.harmattan.ai/cert/rfc2350.pdf.asc

The key used for signing is the team key described in Section 2.8.

---

2. Contact Information

2.1 Name of the Team

CERT Harmattan AI

2.2 Address

Harmattan AI

1 Rue du Mail, 75002 Paris FRANCE

2.3 Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4 Telephone Number

Not available publicly. Reserved for trusted partners.

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication

Secure out-of-band communication channels (e.g. Signal) may be arranged on a per-incident basis. Contact the team via email (Section 2.7) to establish such a channel

2.7 Electronic Mail Address

cert[@]harmattan.ai

This address relays mail to the human(s) on duty. It is monitored during the hours of operation stated in Section 2.11.

2.8 Public Keys and Other Encryption Information

The CERT Harmattan AI has a PGP/GnuPG key for confidential communication:

UID : CERT Harmattan AI

Key ID : 0xF96B83006BAEB54A

Fingerprint : 769D 563B 7AA3 1A52 49EB 578F F96B 8300 6BAE B54A

Key type/size: ed25519

Expires : 2029-06-25

The public key is available from the document location (Section 1.3) and from public key servers. Constituents and partners are strongly encouraged to use this key when sending sensitive information to the team.

2.9 Team Members

A full list of team members is not published for operational security reasons. Individual members will identify themselves during the handling of an incident where appropriate. Management, technical, and operational staff are drawn from Harmattan AI's security function.

2.10 Other Information

General information about Harmattan AI is available at:
https://www.harmattan.ai/

2.11 Points of Customer Contact

The preferred method for reporting an incident to the CERT Harmattan AI is by email to the address in Section 2.7. Encrypted mail using the key in Section 2.8 is encouraged for sensitive content.

Hours of operation: Monday–Friday 09:00–18:00 local time, excluding French public holidays; out-of-hours arrangements for critical incidents.

For incidents affecting deployed Harmattan AI systems in operational environments, escalation paths agreed contractually with the relevant operator take precedence and should be used in addition to the contacts above.

---

3. Charter

3.1 Mission Statement

The CERT Harmattan AI exists to prevent, detect, coordinate and respond to security incidents affecting Harmattan AI, keeping impact and recovery time low and capturing lessons so the same issue doesn't recur.

Our responsibilities:

- Prevent security incidents by implementing security measures and solutions;
- Receive, triage and respond to reported and detected incidents;
- Identify vulnerabilities on our equipment and remediate them;
- Coordinate containment, eradication and recovery, and keep stakeholders informed throughout;
- Monitor for threats and turn detection and intelligence into action;
- Maintain incident records, timelines and post-incident reviews;
- Advise internal teams on prevention and share lessons learned.

3.2 Constituency

The constituency of the CERT Harmattan AI comprises:

- Harmattan AI's corporate information systems, networks, and cloud environments;
- the development, build, and supply-chain infrastructure used to produce Harmattan AI's products;
- the software and hardware products developed by Harmattan AI; and
- Harmattan AI personnel and authorized contractors in their use of Harmattan AI’s information systems.

Incidents involving fielded systems operated by customers are handled in coordination with those operators and according to the relevant contractual and operational agreements.

3.3 Sponsorship and/or Affiliation

The CERT Harmattan AI is established, sponsored, and funded by Harmattan AI. It maintains relationships with relevant Authorities, CSIRT/CERT bodies, sector-specific information-sharing communities, and partner security teams as appropriate.

3.4 Authority

The Harmattan AI CSIRT operates under the authority delegated to it by Harmattan AI management. It is authorized to coordinate the response to information security incidents within its constituency (Section 3.2) and to advise and implement protective measures.

---

4. Policies

4.1 Types of Incidents and Level of Support

The CERT Harmattan AI addresses all types of computer security incidents that occur, or threaten to occur, within its constituency. These include, but are not limited to: unauthorized access, malicious code, denial-of-service, compromise of credentials, data exposure, supply-chain compromise, and vulnerabilities affecting Harmattan AI systems or products.

The level of support given varies according to the type and severity of the incident, the type of constituent affected, the size of the affected community, and the resources available at the time. Incidents are prioritized according to their assessed impact. The CSIRT is committed to keeping its constituency informed of developments where it is appropriate to do so.

4.2 Co-operation, Interaction and Disclosure of Information

The CERT Harmattan AI cooperates with other teams, organizations, and authorities as necessary to resolve incidents, while protecting the interests and information of Harmattan AI, its constituents, and its customers.

Information is shared on a need-to-know basis. The team applies the **Traffic Light Protocol (TLP)** to information it exchanges, and expects correspondents to do the same. Information received in confidence is handled accordingly and is not disclosed outside the team without the originator's consent, except where required by law or by an overriding security need.

Given the defense context in which Harmattan AI operates, the disclosure of certain information may be subject to additional legal, contractual, and export control restrictions; the CSIRT will observe these in all of its interactions.

Anonymized technical information, such as IOCs (Indicator of compromise) or TTPs (TTP (Tactiques, Techniques et Procédures) may be shared with trusted cybersecurity communities and networks as part of coordinated information-sharing efforts, in accordance with the applicable TLP marking.

4.3 Communication and Authentication

For routine communication, email is acceptable. For the exchange of sensitive information, the CSIRT requires the use of encryption with the PGP/GnuPG key described in Section 2.8, and/or other mutually agreed secure channels.

Where the identity of a correspondent must be established, the CSIRT may use PGP signatures, telephone callback to known numbers, or other agreed methods of authentication.

The Information Sharing Traffic Light Protocol (TLP) should be used for any information exchange with CERT Harmattan AI.

---

5. Services

5.1 Incident Response

The CERT Harmattan AI assists its constituency in handling the technical and organizational aspects of incidents. It provides the following components of incident response.

5.1.1 Incident Triage

- Determining whether an incident is genuine;
- assessing and prioritizing the incident according to its scope and severity.

5.1.2 Incident Coordination

- Determining the systems, parties, and information involved;
- coordinating with affected system owners, other internal functions, and, where relevant, external teams, vendors, customers, and authorities;
- facilitating communication among the parties involved while protecting sensitive information;
- maintaining a record of the incident and its handling.

5.1.3 Incident Resolution

- Advising affected parties on containment, eradication, and recovery;
- assisting in collecting and preserving evidence where appropriate;
- conducting or supporting post-incident analysis and capturing lessons learned to reduce the likelihood and impact of future incidents.

5.2 Proactive Activities

In addition to reactive incident response, the CERT Harmattan AI may, subject to available resources, provide proactive services such as:

- issuing security advisories and alerts to its constituency;
- perform security scanning and security audit of its constituency;
- supporting vulnerability handling and coordinated disclosure for Harmattan AI products;
- monitoring for threats relevant to the constituency;
- promoting security awareness and good practice; and
- advising on security configuration and architecture, as well as directly implementing these best practices.

---

6. Incident Reporting Forms

The CERT Harmattan AI does not currently require a specific incident reporting form. When reporting an incident, please include as much of the following as is available:

- contact details and organizational affiliation of the reporter;
- the systems, services, or products affected;
- the nature of the incident and the symptoms observed;
- relevant timestamps (with time zone);
- IP addresses, hostnames, file hashes, log excerpts, or other indicators;
- actions already taken; and
- the sensitivity of the report and any TLP marking that should be applied.

Reports should be sent to the address in Section 2.7, encrypted with the key in Section 2.8 where the content is sensitive.

---

7. Disclaimers

While every precaution is taken in the preparation of information, notifications, and alerts, the CERT Harmattan AI assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein. The CERT Harmattan AI may amend this document at any time; the authoritative version is the one published at the location given in Section 1.3