ERIUM CERT

RFC 2350

Version 1.0

2024.04.15

1 Document Information

1.1 Date of Last Update

Version 1.0, updated 2024.04.15

1.2 Distribution List for Notifications

There is no distribution list for changes to this document.

1.3 Locations where this Document May Be Found

The current version of this document may be found at:

https://www.erium.fr/wp-content/uploads/2024/04/ERIUM-CERT-RFC_2350.pdf

1.4 Authenticating this Document

This document has been signed with the PGP key of ERIUM CERT. The signature and our public PGP key (ID and fingerprint) are available on our website:

https://www.erium.fr/cert

2 Contact Information

2.1 Name of the Team

ERIUM CERT

Subteams:

- Computer Security Incident Response Team (CSIRT)
- Product Security Incident Response Team (PSIRT)

2.2 Address

ERIUM CERT

13 rue du Quatre-Septembre

75002 Paris

France

2.3 Time Zone

Our team works in France and keeps to these hours: CET/CEST

2.4 Telephone Number

None available.

2.5 Facsimile Number

None available.

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 ERIUM, please contact us at: CERT(at)ERIUM(dot)fr.

Other aliases are:

- CSIRT: CSIRT(at)ERIUM(dot)fr
- PSIRT: PSIRT(at)ERIUM(dot)fr

This relays email to the human(s) on duty for ERIUM CERT.

2.8 Public Keys and Encryption Information

The details of the ERIUM CERT PGP public key are:

- Key UID: CERT ERIUM <cert@erium.fr>
- Key ID: 0xCC341FB60D831FEC
- Key fingerprint: D03D 4559 9276 921C E07A 0793 CC34 1FB6 0D83 1FEC
- Sub-key (signing) ID: 0xF55CA7CF66D8D5D9
- Sub-key (signing) fingerprint: BF76 2BA6 503D A882 1AEE 7324 F55C A7CF 66D8 D5D9

Full details can be found on the following page: https://www.erium.fr/cert

2.9 Team Members

The ERIUM CERT team representatives are:

- Primary representative: Pierre Texier <CERT(dot)texier(at)ERIUM(dot)fr>

- Secondary representative: Olivier Caleff <CERT(dot)caleff(at)ERIUM(dot)fr>

The list of the other team members is not publicly available.

2.10 Operating hours

09:00 to 18:00, Monday to Friday for routine communication.

Saturday, Sunday, and days off for France: on-call for CERT customers.

On-call for off-business days or hours on request.

2.11 Other Information

None available.

2.12 Points of Customer Contact

ERIUM prefers to receive vulnerabilities information, incident reports or first level support by email directed to ERIUM CERT's email addresses detailed in Section 2.7. Please use our cryptographic key to ensure integrity and confidentiality.

Other CSIRT and PSIRT related communications can be directed to respective ERIUM CERT's email addresses detailed in Section 2.7.

3 Charter

3.1 Mission Statement

ERIUM is committed to maintaining the confidentiality, integrity, and availability of both its platform and the intellectual property and personal information of its users, customers, and employees.

In order to ensure these principles are upheld, ERIUM maintains security watch, vulnerability management, incident response, and threat hunting capabilities.

3.2 Constituency

Our constituency is composed of:

- ERIUM employees, working in its premises or remote, in the countries it is established: France and Italy
- ERIUM products

- Any organization that uses an ERIUM product or service

Some examples of ERIUM products and services are:

- BlackNoise
- Cyber Investigation

3.3 Sponsorship and/or Affiliation

ERIUM CERT is a team within ERIUM.

Funding is provided by ERIUM.

3.4 Authority

ERIUM CERT operates under the authority of the Chief Security Officer of ERIUM.

4 Policies

4.1 Types of Incidents and Level of Support

ERIUM CSIRT team is authorized to address all types of computer security incidents which occur, or threaten to occur, within its constituency.

ERIUM PSIRT team is authorized to address all types of security incidents related to its products which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident, the number of affected entities within our constituency, and ERIUM resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

ERIUM CERT takes every effort to safely and securely share information with affected parties during incident response situations while respecting the privacy and trust of our constituents.

4.3 Communication and Authentication

ERIUM CERT makes use of the Traffic Light Protocol (TLP) for information sharing.

Email is the preferred method of communication. All sensitive information should be encrypted using the ERIUM CERT PGP key (as detailed in Section 2.8) prior to sending.

5 Services

5.1 Incident Response

ERIUM CERT's CSIRT team is responsible for incident response internally at ERIUM where at least one member of the constituency is affected.

ERIUM CERT's CSIRT team also provides incident response services for customers. Every effort is made to provide timely and accurate information during security incidents to affected customers so they can conduct their own investigations and respond appropriately. See section 2.11 for customer points of contact.

ERIUM CERT's PSIRT team is responsible for incident response related to ERIUM products when they are affected.

5.1.1 Incident Triage

ERIUM CERT carries out the following activities for incident triage:

- Security signals are collected and interpreted to determine risk, severity, and priority.
- Investigation as to whether an incident occurred and what its effect and impact was.

This list is not exhaustive.

5.1.2 Incident Coordination

ERIUM CERT carries out the following activities for incident coordination:

- Situational awareness and analysis for stakeholders teams.
- Command role with authority to direct resources as required.
- External coordination with affected or involved third-parties.

This list is not exhaustive.

5.1.3 Incident Resolution

ERIUM CERT carries out the following activities for incident resolution:

- Engages relevant internal teams to eradicate, restore, and secure.

- Collection and storage of evidence for internal use as well as potential law enforcement involvement.
- Notification to affected constituents.
- Postmortem authoring with lessons learned and post-incident repair items.

This list is not exhaustive.

5.2 Proactive Activities

ERIUM CERT develops, maintains, and operates threat hunting and detection tools and techniques to proactively identify risks and threats.

Work is also done on education, preparation, workflow development, and community outreach.

5.3 Service Areas (CSIRT Services Framework)

The following services areas are covered by ERIUM CERT's CSIRT team:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

CSIRT Services Framework version 2.1 is available at:

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

5.4 Service Areas (PSIRT Services Framework)

The following services areas are covered by ERIUM CERT's PSIRT team:

- Stakeholder Ecosystem Management
- Vulnerability Discovery
- Vulnerability Triage and Analysis
- Remediation
- Vulnerability Disclosure
- Training and Education

PSIRT Services Framework version 1.1 is available at:

https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

6 Incident Reporting Forms

None available. Please review Section 2.11 for reporting guidance.

7 Disclaimers

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

If you see something wrong or unclear in this document, please contact ERIUM CERT at one of the email addresses detailed in Section 2.7.