TLP:[WHITE]

CSIRT RFC 2350

Version [1.0] – [29 Maggio 2025]

[CSIRT DIFESACYBER.COM]

Table of Contents

1. Document Information

1.1 Date of Last Update

29 Maggio 2025

1.2 Distribution List for Notifications

E-mail notifications of updates are sent to the Trusted Introducer Service for incident response and security teams in Europe https://www.trusted-introducer.org

If you have any question about updates, please send an e-mail to csirt@difesacyber.com

1.3 Locations where this Document May Be Found

https://csirt.difesacyber.com/rfc2350.pdf

1.4 Document Authenticity

Firmato con chiave PGP/GPG Key

2. Contact Information

2.1 Team Name	CSIRT DIFESACYBER.COM
2.2 Address	CSIRT DIFESACYBER.COM – Via della Sicurezza, 1 – 00100 Roma (Italia)
2.3 Time Zone	Central Europe, (GMT+1, and GMT+2 from the last Sunday of March to the last Sunday of October)
2.4 Telephone Number	+39 06 0000 000
2.5 Facsimile Number	None
2.6 Other Telecommunication	None
2.7 Electronic Mail Address	csirt@difesacyber.com
2.8 Public Keys and Encryption Information	http://csirt.difesacyber.com/CISIRT_-_DIFESACYBER.COM_pub.asc
2.9 Team Members	Not disclosed
2.10 Other Information	General information about the CSIRT DIFESACYBER.COM can be found at: https://csirt.difesacyber.com
2.11 Points of Contact	The preferred methods for contacting CSIRT DIFESACYBER.COM are via the form mentioned in section 6 or via email at csirt [at] difesacyber [.] com. The mailbox is monitored during hours of operation. Please use PGP/GPG if you intend to send sensitive information. The CSIRT DIFESACYBER.COM operates 24/7 all year round, a telephone number operating 24/7 has been provided to a restricted group of users.

3. Charter

3.1 Mission Statement

We are the Computer Security Incident Response Team (CSIRT) of DIFESACYBER.COM, Non-profit organization for cooperation and support in the Cyber field for Third Sector Entities (ETS). We offer *incident response, threat intelligence and security assessment to NO PROFIT organizations and ONLUS that deal with volunteering members and conduct proactive research on the entire .it space.*

3.2 Constituency

The costituecy of DIFESACYBER.COM consist of every italian organizzation no profit including employees and assets. DIFESACYBER.COM on protecting and safeguarding the Constituency's infrastructures and services - as well as the confidentiality, integrity and availability of its information assets - from potential threats within the cyberspace, by preventing, containing and neutralizing malicious events both within the Information Technology (IT) and Operational Technology (OT) environments, ensuring tailored cybersecurity assistance

3.3 Sponsorship and/or Affiliation

Aula 28 – STELMILIT – CSIRT Course

3.4 Authority

Not disclosed

4. Policies

4.1 Types of Incidents and Level of Support

CSIRT DIFESACYBER.COM is authorized to address all types of security incidents, which occur, or threaten to occur, within its Constituency (see 3.2).

It does however read and evaluate all types of information sent to it regarding potential security events or incidents.

4.2 Co-operation, Interaction and Disclosure of Information

All requests to CSIRT are handled with great care, regardless of their priority. Confidentiality will be determined according to established practices and standards.

In order to help responding, it is suggested to describe any restrictions applicable on how to use or with whom to share the information sent.

As CSIRT DIFESACYBER.COM supports the Information Sharing Traffic Light Protocol (ISTLP, see https://www.trustedintroducer.org/links/ISTLP-v1.1-approved.pdf), information that comes in with the tags WHITE, GREEN, AMBER or RED are handled accordingly.

4.3 Communication and Authentication

It is suggested to use PGP/GnuPG for communications that contains sensitive information (i.e. classified as “Confidential”).

5. Services

5.1 Incident Response (Triage, Coordination and Resolution)

CSIRT DIFESACYBER.COM is responsible for the coordination of security incidents in our constituency and ensures that the information is passed inside the constituency to the responsible persons able to resolve the reported issues.

5.1.1 Incident Triage

Incident triage is handled by CSIRT DIFESACYBER.COM

5.1.2 Incident Coordination

Incident coordination is handled by CSIRT DIFESACYBER.COM. Description of the Incident Coordination is provided in detail within ISO27001 internal procedures.

5.1.3 Incident Resolution

Incident resolution is handled by CSIRT DIFESACYBER.COM in cooperation with the involved constituents. Description of the Incident Management Process is provided in detail within ISO27001 internal procedures.

5.2 Proactive Activities

CSIRT DIFESACYBER.COM performs the following activities for its constituency:

- Security monitoring

- Awareness and information sharing

- Trend and threat analysis

6. Incident Reporting Forms

A public web page for reporting Security Incidents is available at the following URL:

https://csirt.difesacyber.com/segnala-incidenti.html

When reporting incidents, please provide as much information as possible.

For example:

- Type of incident (malicious code, compromised systems, information gathering, etc.)

- Time and date of all events reported. Also include the time zone to help CSIRT DIFESACYBER.COM correlating your information with ongoing incidents.

- If the incident is correlated to malicious code, please contact us by email to agree a secure way to transfer the relevant data to avoid any problem with network based anti-virus tools and intrusion protection systems. Please make sure to always include your own contact information.

7. Disclaimers

The CSIRT DIFESACYBER.COM is not responsible for any misuse of the information contained herein.