cyna
secure your future

RFC 2350

Document information

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

Date of Last Update

- Version 1.0, published on 2023-09-08.

Distribution List for Notifications

- Notifications of updates are submitted to our mailing list when appropriate.

Locations where this Document May Be Found

- The current and latest version of this document is available at Cyna's website at: https://www.cyna-it.fr/réponse-à-incident

Authenticating this Document

- This document has been signed with the PGP key of CynaCSIRT. The signature and our public PGP key (ID and fingerprint) are available on our website: https://www.cyna-it.fr/réponse-à-incident

Document Identification

- Title: 'RFC2350 – CynaCSIRT' Version: 1.0
- Document Date: 2023-09-08

Contact information

Name of the Team

- CynaCSIRT

Address

- 10 rue de Penthièvre, 75008 PARIS FRANCE

Time Zone

- CET/CEST

Telephone Number

- Main number on-call duty: +33 9 70 70 41 81

Facsimile Number

- Not applicable.

Electronic Mail Address

- cert@cyna-it.fr

Other Telecommunication

- Not applicable.

Public Keys and Encryption Information

- PGP is used for functional exchanges with CynaCSIRT.

  - User ID: CynaCSIRT (cert@cyna-it.fr)
  - Key ID: 0x327487D6
  - Fingerprint: F4EC 02C7 B808 28E0 AD10 6E86 56AA CB31 3274 87D6

The public PGP key is published in the following PGP directory: https://keys.openpgp.org/.

Team Members

- The CynaCSIRT team consists of IT security experts, whose specific members are not publicly disclosed. The identities of these team members could potentially be revealed on a case-by-case basis, adhering to need-to-know restrictions.

Points of Customer Contact

- CynaCSIRT encourages its customers to submit incident reports by phone at **+33 9 70 70 41 81** Alternatively, for those who are not customers of CynaCSIRT, the preferred method for submitting incident reports is through email at cert@cyna-it.fr.

We strongly recommend utilizing our cryptographic key to ensure the highest levels of confidentiality and communication integrity. In case of an emergency, kindly insert the [URGENT] tag in the email's subject line. Please note that while CynaCSIRT operates 24/7, telephone support is not available during non-business hours.

Charter

Mission Statement

The primary objective of CynaCSIRT is twofold: firstly, to aid Cyna's customers in proactively implementing measures that mitigate the risks of computer security incidents, and secondly, to support these customers in effectively responding to any such incidents as and when they arise.

CynaCSIRT's mission encompasses prevention, response, and recovery through the following actions:

- Assisting in the prevention of security incidents by providing guidance on the implementation of essential protective measures.
- Disseminating information regarding cyber threats to its stakeholders and partners.
- Overseeing incident response, with the option of collaborating with trusted partners if required. Additionally, CynaCSIRT engages in:
- Participation within reliable networks of Computer Security Incident Response Teams (CSIRTs).

Constituency

CynaCSIRT's constituents consist of:

- Customers of Cyna.
- Users, networks, and systems affiliated with Cyna's services.

Affiliation

- CynaCSIRT is part of Cyna.

Authority

- For internal matters, CynaCSIRT operates under the authority of the management of the Cyna company.

- For customer incidents, CynaCSIRT coordinates security incidents on behalf of its constituency, and only at its constituents' request.

Policies

Types of Incidents and Level of Support

- CynaCSIRT is prepared to handle a spectrum of security incidents that arise within its constituency or loom as potential threats. The extent of assistance offered varies according to the nature and severity of the security incident, along with our availability at the time of the incident's occurrence.

Collaboration, Interaction, and Information Sharing

- CynaCSIRT underscores the utmost importance of operational coordination and the exchange of information among CERTs, CSIRTs, SOCs, and similar entities, as well as with other organizations that contribute to the delivery of its services or offer benefits to CynaCSIRT's constituency.
- CynaCSIRT has the capacity to engage in partnerships with other CSIRTs, CERTs, and affected third parties as necessary within the incident or incident response framework. Information received by CynaCSIRT might be shared internally with various teams within Cyna, as well as with cybersecurity service providers and law enforcement agencies, solely on a need-to-know basis.
- Information linked to incidents or vulnerabilities that could lead to the identification of a Cyna customer will not be disclosed to external parties.
- Anonymized information, such as Indicators of Compromise (IOCs) and Techniques, Tactics, and Procedures (TTPs), may be shared within cybersecurity communities to enhance comprehension of threats, fortify prevention measures, and bolster investigative efforts.

Communication and Authentication

- It is recommended that all emails directed to CynaCSIRT be signed using PGP. For emails containing sensitive information, encryption and PGP signing are imperative. CynaCSIRT adheres to the Information Sharing Traffic Light Protocol, as established by the French national cybersecurity agency (ANSSI TLP).

Services

Incident Response

- CynaCSIRT offers 24/7 incident response services to our constituents. We assess all incidents related to information and communication technologies. Our team of technical experts conducts thorough and in-depth analysis.

Incident Triage

- Severity Evaluation
- Expert Escalation
- Strategic Leadership

Incident Coordination

- Data Classification
- Selective Notification
- Real-time Channels
- Incident Playbooks
- Team Collaboration
- Communication Updates

Incident Resolution

- Forensic Analysis and Investigation
- Vulnerability Remediation
- Malware Eradication
- Recovery and Rebuilding
- Threat Hunting
- Lessons Learned and Analysis
- Continuous Monitoring and Threat Intelligence Integration
- Stakeholder Communication and Reporting
- Policy and Procedure Refinement
- Training and Awareness

Proactive Cybersecurity Measures

Cyna is committed to delivering proactive cybersecurity services to its clients, encompassing a range of strategic actions such as:

- Security Operation Center detection Services & Capabilities
- Asset Vulnerability Scans
- Active Directory Security Assessment
- Cloud Service Vulnerability Assessment
- Phishing Awareness Campaigns

These proactive measures underscore Cyna's commitment to staying ahead of emerging cyber threats and ensuring the utmost security for its clientele. For an up-to-date listing of services, please refer to the Cyna website at https://cyna-it.fr.

Incident Reporting Forum

CynaCSIRT's team members have access to an internal form designed to facilitate the systematic collection of essential information when responding to an incident call. However, parties reporting security incidents are not required to use specific forms. If feasible, kindly furnish the subsequent details:

- Contact Information: Please provide your contact details, including email address and phone number.
- Incident Timeline :
  - Start Time: Specify the date and time when the incident commenced.
  - Detection Time: Indicate the date and time when the incident was identified.
- Incident Description: Offer a concise yet comprehensive overview of the incident, including relevant contextual details.
- Affected Assets: Enumerate the systems, networks, or assets directly impacted by the incident.
- Impacts: Detail the consequences and potential ramifications resulting from the incident.
- Actions Taken: Outline any actions already undertaken in response to the incident, such as containment efforts or mitigation strategies.

While the internal form streamlines the process for CynaCSIRT members, parties reporting incidents need not adhere to specific forms. Providing the aforementioned information will greatly aid in the efficient handling of the incident.

Disclaimers

While CynaCSIRT is committed to ensuring accuracy and diligence in the creation of information, notifications, and alerts, it does not accept liability for any errors, omissions, or damages arising from the utilization of the provided information.