Document title

EURONEXT CSIRT

Document type or subject

RFC 2350 OF EURONEXT CSIRT

Revision number	Date
Revision Number: 3.0	2023/06/20

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext's subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext.

Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at www.euronext.com/terms-use.

CONTENTS

ABOUT THIS DOCUMENT

This document describes the Computer Security Incident Response Team (CSIRT) of Euronext N.V. in accordance to RFC 2350. It provides basic information about the Euronext CSIRT team, its channels of communication, and its roles and responsibilities

1.1 DATE OF LAST UPDATE

Version	Date	Author	Comment
1.0	2018/06/07	InfoSec	
2.0	2022/07/15	InfoSec	PGP Key Update
3.0	2023/06/20	InfoSec	PGP Key Renewal

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this document can be found at https://www.euronext.com/RFC2350.

1.4 AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of EURONEXT CSIRT - see section 2.8 for more details on the PGP key.

1.5 DOCUMENT IDENTIFICATION

Title: "RFC 2350 EURONEXT CSIRT"

Version: 3.0 Document

Date: 20 June 2023

Expiration: This document is valid until superseded by a later version

CONTACT INFORMATION

2.1 NAME OF THE TEAM

EURONEXT CSIRT: Euronext Computer Security Incident Response Team

Short name: EURONEXT CSIRT

2.2 ADDRESS:

EURONEXT CSIRT
Av. da Boavista, 3433
4100-138 Porto
PORTUGAL

2.3 TIME ZONE

Time-zone: WET/WEST

2.4 TELEPHONE NUMBER

(+351) 910 124 465

2.5 FACSIMILE NUMBER

None.

2.6 OTHER TELECOMMUNICATION

None.

2.7 ELECTRONIC MAIL ADDRESS

All incident reports should be sent to: security.incident@euronext.com.

All non-incident related email should be addressed to csirt@euronext.com.

Use of phone for reporting incidents should be avoided as much as possible.

2.8 PGP KEY INFORMATION

EURONEXT CSIRT uses PGP for encrypting information in communication with other entities.

KEY ID: 4547BCE28C779F15

KEY Fingerprint: EC2B 063F 9BC8 2C55 C2DA E051 4547 BCE2 8C77 9F15

KEY VALIDITY: 2024-06-19

KEY SIZE: 3072

2.9 TEAM MEMBERS

No public information is provided about EURONEXT CSIRT team members.

2.10 OTHER INFORMATION

None.

2.11 POINTS OF CUSTOMER CONTACT

The preferred method to contact EURONEXT CSIRT team is to send an e-mail to one of the addresses in the Electronic Mail Address section of this document. Urgent cases can additionally be reported by phone to the telephone number identified on the Telephone Number section of this document.

CHARTER

3.1 MISSION STATEMENT

EURONEXT CSIRT provides information and assistance to its constituents (business units, users) in responding to computer security incident, on the imminence of their occurrence or when they occur, along with promoting proactive measures to reduce the risks of computer security incidents at all.

3.2 CONSTITUENCY

The constituency of Euronext CSIRT is composed of all the personnel, services and underlying infrastructure of Euronext N.V. and its subsidiaries.

3.3 SPONSORSHIP AND/OR AFFILIATION

EURONEXT CSIRT is composed of Information Security personnel and from other offices, acting under the authority of the Information Security Office and its Chief Information Security Officer to protect Euronext N.V.

3.4 AUTHORITY

EURONEXT CSIRT is a Euronext N.V. service under the Information Security Office and its Chief Information Security Officer.

POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

All incidents are considered normal priority before internal triage. EURONEXT CSIRT handles all computer security incident types, namely, those that result in a security violation of the following types:

- Data Breach
- Malware
- Availability
- Information Gathering
- Intrusion
- Intrusion Attempt
- Information Security
- Fraud
- Abusive Content
- Vulnerability

Depending on the type, severity and scope of the ongoing incident, adequate support levels are provided.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSIRT EURONEXT recognizes the importance of operational cooperation and information-sharing between CSIRT / CERT teams, and with other organisations which may contribute towards or make use of their services. EURONEXT CSIRT operates within the confines imposed by EU legislation. Sensitive data is only shared with third parties on a need-to-know basis and with the previous authorization of the owner of the information.

4.3 COMMUNICATION AND AUTHENTICATION

EURONEXT CSIRT protects sensitive information in accordance with relevant regulations and policies within the European Union. For non-sensitive information, clear text email or telephone can be used. For sensitive information, the use of PGP is recommended.

SERVICES

5.1 ALERTS AND WARNINGS

This service aims at disseminating information on ongoing (or risk of happening) computer security attacks or disruptions, security vulnerabilities, intrusions, computer viruses and other related security information with the aim to provide guidance and recommendations to the constituent.

5.2 INCIDENT HANDLING

This service aims at the coordination of response to information security incidents in the Euronext N.V. The Incident Handling service (also known as incident management) activities include:

- Determining the impact, scope, and nature of the event or incident;
- Understanding the technical cause of the event or incident;
- Identifying what else may have happened or other potential threats resulting from the event or incident;
- Researching and recommending solutions and workarounds;
- Coordinating and supporting the implementation of the response strategies with other parts of the organization;
- Disseminating information on current threats or attacks, through alerts, advisories or other technical publications;
- Coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement;
- Assure that a proper lesson learned is performed for major incidents or minors (if recurrent);
- Maintaining a repository of incidents and activity related to the constituency that can be used for correlation, trending, and developing lessons learned to improve the security posture and incident management processes of an organization;
- Escalate incidents to Management;
- Communication.

INCIDENT REPORTING FORMS

There are no local forms developed yet for reporting incidents to EURONEXT CSIRT

In case of an emergency or crisis, please provide CSIRT EURONEXT at least with the following information:

- Contact details and organizational information – the name of person and organisation name and address, email address, telephone number;
- IP address and observation time;
- Available evidence showing the problem (logs, screenshots, emails etc.);
- In case of email forwarding, please ensure that all content (headers, body and any attachments) are included.

DISCLAIMERS

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