RFC 2350

CSIRT Pernod Ricard

TLP:CLEAR

Date of publication	06/18/2024
Version	1.1
Author	Cyber Defence Manager
Reviewer	Chef Information Security Officer

Contents

Pernod Ricard
Créateurs de convivialité

Document Information

This document contains a description of CSIRT Pernod Ricard (CSIRT PR) as implemented by RFC2350. It provides basic information about CSIRT PR, its communication channels, its roles responsibilities, and the services offered.

Date of Last Update

Version 1.1 from 18 June 2024.

Distribution List for Notifications

There is no distribution list for notifications.

Locations where this Document May Be Found

The current and latest version of this document is available from [Politique de protection des données personnelles | Pernod Ricard (pernod-ricard.com)]

Authenticating this Document

This document has been signed with the PGP key of CSIRT PR. The PGP public key, ID and fingerprint are available on the Pernod Ricard website.

Document Identification

Title: CSIRT PR RFC 2350
Version: 1.1
Document Date: 2024-06-18
Expiration: this document is valid until superseded by a later version

Contact Information

Name of the Team

Full Name: Pernod Ricard CSIRT
Short Name: PR-CSIRT

Pernod Ricard CSIRT is a Computer Security Incident Response Team for the Pernod Ricard group and brands and subsidiaries.

Address

5, Cours Paul Ricard
75380 Paris CEDEX 08

Time Zone

CET/CEST.

Telephone Number

N/A

Facsimile Number

N/A

Electronic Mail Address

To report an information security incident or a cyber-threat targeting or involving Pernod Ricard group entities, please contact us at the following address: csirt@pernod-ricard.com

Other Telecommunications

N/A

Public Keys and Encryption Information

CSIRT PR uses the following PGP key:

- csirt@pernod-ricard.com
- ID: 2BE5 2CBA 5E36 3CFF
- Fingerprint: AEE3 D4C7 4425 96ED 0D8B C63C 2BE5 2CBA 5E36 3CFF

The key shall be used whenever information must be sent to CSIRT PR in a secure manner.

Team Members

Pernod Ricard CSIRT team is leaded by the Cyber Defense Manager. The team consists of IT security analysts. Neither the size of the team nor the identity of the members is disclosed in this document.

Other Information

N/A

Points of Contact

The preferred method to contact CSIRT PR is by sending an email to the following address: csirt@pernod-ricard.com.

Note: The Preferred language is English. We recommend the use of signature in your message.

Charter

Mission Statement

Pernod Ricard CSIRT (Computer Security Incident Response Team) delivering security services in Pernod Ricard's operation regions. Part of the cybersecurity organization and reporting to the group CISO (Chief Information Security Officer), its main purpose is to assist the company and subsidiaries regarding information system security:

- In centralizing and process assistance request related to cybersecurity event (attacks) on networks & information systems to provide a systematic response.
- In responding to such incidents whenever they occur, by managing alerts with technical analysis and conduct incident response with the stakeholders.
- To minimize incident-based losses, theft of information and disruption of services.
- By participating in communication regarding significative security event, crisis, and through alerting and sensitization.
- To manage and detect tentative of exploit on Pernod Ricard network in collaboration with the Security Operation center.
- In the build and maintenance of a vulnerability database to manage and reduce vulnerability in the information system.
- In the sharing of information with other CERT/CSIRT entities through cybersecurity group memberships.
- And coordination with related third parties: suppliers security teams, government CERT/CSIRT.

Constituency

The constituency of CSIRT PR is composed of all institutions and organizations belonging to the Pernod Ricard Group.

Affiliation

CSIRT PR is affiliated to the Pernod Ricard Group and part of the TECH department. It maintains contacts with various national and international CSIRT and CERT teams according to its needs and the information exchange culture that it values.

Authority

CSIRT PR operates under the authority of the Pernod Ricard Chief Information Security Officer.

Policies

Types of Incidents and Level of Support

PR CISRT manages all types of incidents impacting the confidentiality, integrity or availability of Group Pernod Ricard information systems and processes.

Depending on the incident, CSIRT PR's expertise may cover, but is not limited to the areas of incident response and crise coordination.

Co-operation, interaction, and disclosure of information

PR CISRT exchanges all necessary non-restricted information with other CSIRTs / CERTs as well as with other affected parties involved on in the incident or incident response process.

Incident or vulnerability related information would not be publicly disclosed without the agreement of all involved parties.

Communication and Authentication

CSIRT PR recommend sending all information through signed email or in a secure manner. CSIRT PR supports the FIRST TLP (Traffic Light Protocol) to classify information sharing ability.

Services

Incident response

CSIRT PR offers the following incident response services:
- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response
- Incident coordination

Incident Reporting Forms

To report an external incident from the outside to CSIRT PR, please provide the following details:
- contact details and organizational information such as person or organization's name, address and contact information,
- email address, phone number, PGP key if available,

- reason of contact,
- Any relevant technical element or comment,
- supporting technical elements such as logs to illustrate the issue

Disclaimers

While all precautions are taken in the preparation of information, notifications, and alerts, Pernod Ricard CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.