KERING-CERT RFC 2350

Application date: 01/03/2023

Issued by: Information security team

Contents

Preamble

Kering Group develops an ensemble of luxury brands across every region of the globe. The current, partial, list of Kering Brands is available on http://www.kering.com

1. Document information

This document contains a description of Kering-CERT as recommended by RFC 2350. It provides basic information about Kering-CERT, its channels of communication, its roles, responsibilities, and the services offered.

1.1. Date of last update

Version 1, created on 2022-08-10. Version 1.3 Update on 2023-08-08

1.2. Distribution list for notifications

There is no distribution list for notifications. This document is kept up to date at the location specified in 1.3. Should you have any questions regarding updates, please contact the Kering-CERT Team at the email address mentioned below.

1.3. Locations where this document may be found

The current and latest version of this document is available on the Kering's Cybersecurity Portal at the following URL:

https://www.kering.com/api/download-file/?path=KERING_CERT_RFC_2350_public_e1ed45c0db.pdf

Please make sure you are using the latest version.

1.4. Authenticating this Document

This document has been signed with the Kering-CERT PGP key.

The integrity of the document can be verified using PGP.

1.5. Document Identification

Title: Kering-CERT RFC 2350

Version: 1.3

Document Date: 2023-08-08

Expiration: This document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team

Full Name: Kering-CERT

Short Name: Kering-CERT

Kering-CERT is a computer Emergency Response Team and a Computer Security Incident Response Team for the Kering group, houses and brands and subsidiaries.

2.2. Address

KERING
CERT
37 RUE DU CHERCHE MIDI
75006 PARIS
FRANCE

2.3. Time Zone

GMT+1 (with Daylight Saving Time or Summertime, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as CET/CEST.

2.4. Telephone Number

An on-call phone number is available 24/7, restricted to Internal use only.

[redacted]

2.5. Facsimile Number

Facsimile is not available.

2.6. Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Kering, please contact us at:

cert@kering.com

2.7. Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the Kering-CERT has a PGP key:

- KeyID: EC88 7AA0 E6CE DCDE
- Fingerprint: 9ACD17607DBBDC17C8CE1CADEC887AA0E6CEDCDE

The key can be retrieved from one of the usual Kering websites such as:

[redacted]

The key can be found bellow:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID: Kering CERT <cert@kering.com>
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User-IDs
Comment: Fingerprint: 9ACD17607DBBDC17C8CE1CADEC887AA0E6CEDCDE

mDMEYw4JxRYJKwYBBAHaRw8BAQdAvvoia6dA7dbEAkHIwagjPrPkIch+QfV4OpTi
Tti54cu0HUtlcmluZyBDRVJUIDxjZXJ0QGtlcmluZy5jb20+iJMEExYKADsWIQSa
zRdgfbvcF8jOHK3siHqg5s7c3gUCYw4JxQIbAwULCQgHAgIiAgYVCgkICwIEFgID
AQIeBwIXgAAKCRDsiHqg5s7c3nfYAQC3mbx3+LU3sHtYxjbmwAcyWkqy0zTLipnb
eF4lsOk2owD+J4vDhikyre7XwbxHvfJnD3J3+QluGhW7xU3W+BCmUAK4OARjDgnF
EgorBgEEAZdVAQUBAQdA08htWGU0Pmpop6xRSFD26hCrPFF0olznwN/IoNmkfRUD
AQgHiHgEGBYKACAWIQSazRdgfbvcF8jOHK3siHqg5s7c3gUCYw4JxQIbDAAKCRDs
iHqg5s7c3rqHAP42ckUZLPgWopLFxVKAT3pcsncwqVWmMUH8wYaniHr6LgD/WVbr
ZQE7ymYrFniZmTkQqmTstqyRa7wakghx4HATNQI=
=/Vd8
-----END PGP PUBLIC KEY BLOCK-----
```

The key shall be used whenever information must be sent to Kering-CERT in a secure manner.

Please use this key when you want/need to encrypt messages that you send to Kering-CERT.

- When due, Kering-CERT will sign messages.
- When due, sign your messages using your own key please. It helps when that key is verifiable (for instance, using the public key servers).

2.8. Team Members

Kering-CERT’s acting team leader is Etienne LADENT, also acting as Representative.

The team consists of IT security analysts. Neither the size of the team nor the identity of the members is disclosed in this document.

2.9. Other Information

General information about Kering-CERT can be found on the Kering Cybersecurity portal:

---internal use only---

2.10. Points of Contact

The preferred method to contact Kering-CERT is to send an email to the following address:

cert@kering.com

Preferred language is English, we recommend the use of encryption in your message (cf. *§2.7 - Public Keys and Encryption Information*). If necessary, urgent cases can be reported by phone (cf. *§2.4 - Telephone Number*) during French business hours. Kering-CERT's hours of operation are 24/7.

2.11. Emergency contact

In case of emergency - and only in this case, e.g. if the previous points of contact are unavailable for any reason - an alternate method to contact the Kering-CERT is to send an email to the following address:

cert@kering-cert.com

3. Charter

3.1. Mission Statement

Kering-CERT mission statement is specified in a dedicated "CSIRT Mandate" document available on the Kering's Cybersecurity portal and bellow for easy reading.

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

- In implementing proactive measures to reduce the company exposure regarding cybersecurity risks, prepare future incidents management and provide optimized protection.
- In the prevention of incidents by working with compliance, privacy, and protection teams to diminish risks their occurrences, or consequences.
- 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.
- 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.

Kering-CERT oversees DFIR (Digital Forensics and Incident Response) activities. The scope of Kering-CERT activities covers prevention, detection, investigation, response, and recovery.

Kering-CERT members are driven by several key values:

- Kering-CERT strives to act according to the highest standards of ethics, integrity, honesty, and professionalism.

- Kering-CERT is committed to deliver a high-quality service to its constituency.
- Kering-CERT will ensure to respond to security incidents as efficiently as possible.
- Kering-CERT will maintain a high-level set of skills.
- Kering-CERT will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

Detailed information about the Kering-CERT activities, service levels, and missions are specified in the RFC2350 document published and keep up to date on the Kering CyberSecurity Portal.

Kering-CERT mission is to support the company, its houses, subsidiaries, and key partners to protect themselves against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests.

3.2. Constituency

Kering-CERT's primary constituency is composed of all the elements of Kering Information System: its users, its systems, its applications, and its networks.

However, Kering-CERT's services are also delivered to a secondary constituency : subsidiaries and houses.

Any entity in the Kering organization can benefit from Kering-CERT's services.

3.3. Affiliation

Kering-CERT is affiliated to Kering Group in France, and part of Kering Technology.

It maintains contacts with various national and international CSIRT and CERT teams according to its needs and the information exchange culture that it values.

3.4. Authority

Kering-CERT operates under the auspices of, and with authority delegated by, the Kering group.

Kering-CERT coordinates security incidents on behalf of its constituency. Kering-CERT have authority to require specific actions during incidents.

Kering-CERT primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Generally, Kering-CERT expects to work co-operatively with its constituents like system administrators and users.

4. Policies

4.1. Types of Incidents and Level of Support

Kering-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, in the constituency networks.

The level of support given by Kering-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and Kering-CERT's resources at the time. Regarding the security incident's type, Kering-CERT will provide a response within two working days. Incidents will be prioritized according to their apparent severity and extent, which could impact services response delay.

End users are expected to contact their End user support, systems administrator, network administrator, or manager for assistance before reaching out to Kering-CERT.

4.2. Co-operation, interaction, and disclosure of information

Kering-CERT exchanges all necessary information with other SOC, CSIRT and CERT as well as with affected parties' administrators. These operational coordination and information sharing are considered as high value which may help to deliver the services and provide benefits to Kering-CERT's constituency.

Moreover, Kering sends its members to cybersecurity events: conferences, exhibitions, working groups, etc.

Neither personal nor stakeholder data are exchanged unless explicitly authorized. All sensitive data (such as personal data, system configurations, known vulnerabilities with their locations) are shared on a need-to-know basis and encrypted if they must be transmitted over unsecured environment as stated below.

Kering-CERT operates within the current French legal framework.

4.3. Communications and Authentication

Kering-CERT protects sensitive information in compliance with relevant French and European regulations and policies within France and the EU. Kering-CERT respects the sensitivity markings allocated by originators of information communicated to Kering-CERT (“originator control”).

Kering-CERT supports the Information Sharing Traffic Light Protocol version 2.0 (https://www.first.org/tlp/) and will handle appropriately information tagged with it.

Communication security (which includes both encryption and authentication) is achieved using GPG primarily or any other agreed means, depending on the sensitivity level and context.

In view of the types of information that Kering-CERT deals with, telephones are considered secure enough to be used for non-sensitive information and unencrypted emails are authorized for the transmission of low-sensitivity data.

For sensitive audio communication, encrypted tools should be used.

Similarly, to send sensitive data by e-mail, encryption (preferably GPG) will be used. Network file transfers must be encrypted just like emails and sensitive data.

5. Services

Service are described based on the definition of the First (CSIRT) Services Framework[1].

5.1. Information Security Event Management

Kering-CERT handles both the triage, resolution, and coordination aspects. Kering-CERT performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks and regarding of the compliance level of systems and applications with the Kering’s security policies.

It coordinates and maintains the following services to the extent possible depending on its resources, and will assist or advice in the following aspects of incidents management

- Monitoring and detection
  - Log and sensor management
  - Detection use case management
  - Contextual data management
- Event analysis
  - Correlation
  - Qualification

5.2. Information Security Incident Management

Kering-CERT will assist stakeholder and system administrators in handling the technical and organizational aspects of incidents. Depending on the incident scope, incident resolution may be left to the responsible administrators within the constituency. In any case, Kering-CERT will offer support and advice on request.

- Information security incident report acceptance.

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

  - Information Security Incident Report Receipt
  - Information Security Incident Triage and Processing
- Information security incidents analysis
  - Information security incident triage (prioritization and categorization)
  - Information collection
  - Detailed analysis coordination
  - Information security incident root cause analysis
  - Cross-incident correlation
- Artefact and forensic evidence analysis
  - Media or surface analysis
  - Reverse engineering
  - Runtime and/or dynamic analysis
  - Comparative analysis
- Mitigation and recovery
  - Response plan established
  - Ad hoc measures and containment
  - Systems restoration
  - Other information security entities support
- Information security incident coordination
  - Communication
  - Notification distribution
  - Relevant information distribution
  - Activities coordination
  - Reporting
  - Media communication
- Crisis management support
  - Information distribution to constituents
  - Information security status reporting
  - Strategic decisions communication

5.3. Vulnerability Management

Kering-CERT will propose a vulnerability watch and remediation service, following the service description bellow.

- Vulnerability discovery / research
  - Incident response vulnerability discovery
  - Public source vulnerability discovery
  - Vulnerability research
- Vulnerability report intake
  - Vulnerability report receipt
  - Vulnerability report triage and processing
- Vulnerability analysis

  - Vulnerability triage (validation and categorization)
  - Vulnerability root cause analysis
  - Vulnerability remediation development
- Vulnerability coordination
  - Vulnerability notification/reporting
  - Vulnerability stakeholder coordination
- Vulnerability disclosure
  - Vulnerability disclosure policy and infrastructure maintenance
  - Vulnerability announcements/communication/dissemination
  - Post-vulnerability disclosure feedback
- Vulnerability response
  - Vulnerability detection / scanning
  - Vulnerability remediation

5.4. Situational Awareness

Kering-CERT will collect statistics on the incidents dealt and may notify the constituency as necessary to assist them in protecting against known attacks.

- Data acquisition
  - Policy aggregation, distillation, and guidance
  - Asset mappings of assets to functions, roles, actions, and key risks
  - Collection
  - Data processing and preparation
- Analysis and synthesis
  - Projection and inference
  - Event detection (through alerting and/or hunting)
  - Situational impact
- Communication
  - Internal and external communication
  - Reporting and recommendations
  - Implementation
  - Dissemination / integration / information sharing
  - Management of information sharing

5.5. Knowledge Transfer

Kering-CERT disseminates information on cyberattacks, disruptions, security vulnerabilities, alerts, malware, and provides recommendations to tackle the issue within its constituency. Alerts and warnings may be fowarded on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

Kering-CERT may provide information on the threat landscape, published vulnerabilities, new attack tools or artefacts and security measures. Perform training and educational services.

Kering-Cert also maintains Information services such as: list of security contacts, repository of security-related patches for various operating systems.

Kering-CERT develops security tools for its own use, to improve its services and support its activities as needed. These tools may be shared with the cybersecurity community, privately or publicly.

- Awareness building
  - Research and information aggregation
  - Report and awareness materials development
  - Information dissemination
  - Outreach
- Training and education
  - Knowledge, skill, and ability requirements gathering
  - Educational and training materials development
  - Content delivery
  - Mentoring
  - CSIRT staff professional development
- Exercises
  - Requirements analysis
  - Format and environment development
  - Scenario development
  - Exercises execution
  - Exercise outcome review
- Technical and policy advisory
  - Risk management support
  - Business continuity and disaster recovery planning support
  - Policy support
  - Technical advice

6. Incident Reporting Forms

Incident report template has been developed to report incidents to Kering-CERT.

To report a cybersecurity incident to the team, please contact the End User Support.

In case of emergency or crisis, please provide Kering-CERT at least the following information:

  - Incident Short description
  - Contact details and organizational name, including address, email, PGP keys, and telephone number
  - Date and time when the incident started and when the incident was detected.
  - Severity and urgency
  - Possible impacts
  - Affected assets (brands, regions, users & machines lists, etc.)
  - Incident detailed description with technical data, if possible.
  - Indicators of compromise: date, IP, ports, URL, software, hash, file name, email subject or attachements
  - Actions taken so far with timestamps.

- Expectations or priorities.

7. Disclaimers

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

If you found any error, please inform us by email at cert@kering.com.