TLP:CLEAR

EL_CSIRT_RFC2350

[October 3, 2023]
Version: 1.0 – **Initial version**

Index :

1. Document information.

This document contains a description of the EL-CSIRT in accordance with RFC 2350 specification. It provides basic information and describes its responsibilities and services offered.

1.1 Date of last update.

Version 1.0, published on 2023-10-03.

1.2 Distribution list for notifications.

There is no distribution list set to notify on modifications to this document.

1.3 Locations where this document may be found.

The EssilorLuxottica CSIRT - RFC2350 document is available on our Ethics and Compliance webpage https://www.essilorluxottica.com/en/governance/ethics-and-compliance/

1.4 Authenticating this document.

This document has been signed with the PGP key of EL-CSIRT. The signature of the EssilorLuxottica CSIRT - RFC2350 document is available on our Ethics and Compliance webpage https://www.essilorluxottica.com/en/governance/ethics-and-compliance/

1.5 Document identification.

Title: "EL_CSIRT_RFC2350"
Version: 1.0
Document Date: 2023-10-02
Expiration: this document is valid until superseded by a later version.

2. Contact information.

2.1 Name of the team.

Official Name: EssilorLuxottica Computer Security Incident Response Team.
Short Name: EL-CSIRT.

2.2 Address.

EssilorLuxottica Group
Piazzale Luigi Cadorna, 3
20121 Milano MI
Italy

2.3 Time Zone.

CET/CEST.

2.4 Telephone Number.

+1 325 307 1014

2.5 Electronic Mail Address.

To report an information security incident or a cyber-threat targeting or involving Essilor Luxottica entities, please contact us at the following address: csirt@essilorluxottica.com.

2.6 Public keys and Encryption Information.

PGP is used for functional exchanges with EL-CSIRT.

- User ID: EL-CSIRT <csirt@essilorluxottica.com>
- Key ID: 0x34519DE5
- Fingerprinting : C6BF C17D 857C A3D5 77D7 5651 4CE8 F3C1 3451 9DE5

The public PGP key can be retrieved from this public key server https://pgp.circl.lu/.

2.7 Team members.

EL-CSIRT team is composed of IT security experts. The list of EL-CSIRT team's members is not publicly available. The identity of EL-CSIRT team's members might be divulged on a case-by-case basis according to the need-to-know restrictions.

2.8 Points of Contact.

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

3. Charter.

3.1 Mission Statement.

The activities of EL-CSIRT are non-profit and are financed by EssilorLuxottica group. The mandate for EL-CSIRT is as follows:

- Identifying and anticipating cyber threats through a recurring monitoring activity on cyber threats and vulnerabilities for the entire EssilorLuxottica Group and its subsidiaries.

- Protecting the EssilorLuxottica Group and its subsidiaries from cyber threats using several security tools and by delivering several cybersecurity services.

- Detecting, responding, and coordinating cyber security incidents that may affect EssilorLuxottica assets.

3.2 Constituency.

EL-CSIRT coordinates and processes the response to incidents. It also provides cybersecurity services for the entire EssilorLuxottica Group and its subsidiaries.

3.3 Sponsorship / Affiliation.

EL-CSIRT is a private CSIRT in the Optical & Eyewear Industry sector. It is operated, financed, and owned by the EssilorLuxottica Group.

3.4 Authority.

EL-CSIRT acts under the authority of the EssilorLuxottica Group.

3.5 Responsibility.

EL-CSIRT is responsible for anticipating, protecting, and responding to cybersecurity incidents throughout the EssilorLuxottica Group and its subsidiaries.

4. Policies.

4.1 Types of incidents and level of support.

EL-CSIRT coordinates, analyzes, and handles cybersecurity incidents that could target the EssilorLuxottica Group and its subsidiaries, leveraging its L1, L2 and L3 expertise.

As such, it also participates in the management of cybersecurity vulnerabilities by informing people who need to know about vulnerabilities in products they manage and supporting them to define a remediation plan.

The level of support offered by EL-CSIRT may vary according to the type of incident, its criticality, and the resources available to handle it.

4.2 Co-operation, Interaction and Disclosure of Information.

EL-CSIRT considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, since such cooperative actions are likely to improve EL-CSIRT's efficiency at solving day-to-day problems and specific incidents.

At a Groupwide level, EL-CSIRT is willing to exchange all necessary information with other EssilorLuxottica regional security teams who may be concerned on a need-to-know basis.

No incident or vulnerability will be disclosed publicly without the agreement of all the concerned parties. If not agreed otherwise, supplied information is kept confidential.

Legal requests will be evaluated by our Legal Department and an appropriate response will be given if the request is acceptable, within the limits of the court order, the related investigation and the information requested.

4.3 Communication and authentication.

A preferred method of communication is email. By default, all sensitive communication to EL-CSIRT should be encrypted with our public PGP key detailed in Section 2.6.

EL-CSIRT also recognizes and follows the FIRST TLP (https://www.first.org/tlp/) version 2.0.

5. Services.

5.1 Incident response.

EL-CSIRT is in charge of responding to any cybersecurity event impacting EssilorLuxottica Group and its subsidiaries.

According to the extent of the security incident, EL-CSIRT takes over the lead and manages containment, analysis and recommend remediation actions with the support of system administrators and business managers.

To this aim, it provides different incident response services on 24/7:

- Incident triage: Confirm if the security event report is a relevant security incident and perform a first assessment.

- Incident coordination: Determine the priority of the incident and if needed set up crisis meetings with IT and business managers. Liaise with legal, communication if necessary. Communicate with other external parties if relevant.

- Incident investigation: Digital forensics analysis of compromised systems.

- Incident resolution: Follow Patching/Hardening/Recovery activities until security risk dropdowns. Provision IOCs to detect and block abnormal activities. Recommend security improvements to system administrators and business managers by providing a remediation plan.

5.2 Intrusion detection.

EL-CSIRT leverages tools, services, and processes to detect potential intrusions targeting the EssilorLuxottica Group and its subsidiaries on 24/7.

5.3 Pre-emptive Security Controls.

EL-CSIRT performs pre-emptive security controls to detect potential breaches, vulnerabilities and misconfigurations that may be leveraged by threat actors. These security controls tend to align the compliance level of various systems and applications with the existing security policies.

6. Incident reporting.

To report an incident, please report the incident by encrypted email to the address in section 2.5.

Incident reports should contain the following information:

- Date and time of the incident (including time zone).
- Description of the incident.
- Source/Destination IPs, ports and protocols or products concerned.
- Any other relevant information.

7. Disclaimers.

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