SOCIETE GENERALE

RFC 2350

CERT Société Générale

Date of publication	2018-11-08
Version	1.0
Author	Alex KOUZMINE
Reviewer	Olivier BERNI

TABLE OF CONTENTS

1 - Diffusion

TLP:WHITE

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:WHITE information may be distributed without restriction, subject to copyright controls.

2 - Document Information

This document contains a description of CERT Société Générale (CERT SG) as implemented by RFC 2350. It provides basic information about CERT SG, its communication channels, its roles and responsibilities.

2.1 Date of Last Update

Version 1.0 from November 8, 2018.

2.2 Distribution List for Notifications

There is no distribution list for notifications.

2.3 Locations where this Document May Be Found

The current and latest version of this document is available from CERT SG's website at: https://cert.societegenerale.com/CERT_SG_RFC2350.pdf

2.4 Authenticating this Document

This document has been signed with the PGP key of CERT SG. The signature is available from CERT SG's website at:
https://cert.societegenerale.com/CERT_SG_RFC2350.pdf.sig

2.5 Document Identification

Title: CERT SG RFC 2350
Version: 1.0
Document Date: 2018-11-08
Expiration: this document is valid until superseded by a later version

3 - Contact Information

3.1 Name of the Team

CERT SG: CERT Société Générale

3.2 Address

CERT SG
Société Générale
189 rue d'Aubervilliers
75886 PARIS CEDEX 18
FRANCE

3.3 Time Zone

CET/CEST

3.4 Telephone Number

+33 1-5898-7200 (24/7)

3.5 Facsimile Number

N/A

3.6 Electronic Mail Address

To report an information security incident or a cyber-threat targeting or involving Société Générale Group entities, please contact us at the following address:

cert.sg@socgen.com

3.7 Other Telecommunications

N/A

3.8 Public Keys and Encryption Information

CERT SG uses the following PGP key:

- ID: 0xB71A3D14
- Fingerprint: 3491 6594 949E A60A D7B7 6FB2 6461 28CB B71A 3D14

The key can be retrieved at any time from applicable public key servers such as https://pgp.circl.lu/. The key shall be used whenever information must be sent to CERT SG in a secure manner.

3.9 Team Members

CERT SG team leader is Olivier BERNI. The team consists of IT security analysts.

3.10 Other Information

Additional applicable information about CERT SG can be found at the following address: https://cert.societegenerale.com

3.11 Points of Contact

The preferred method to contact CERT SG is by sending an email to the following address: cert.sg@socgen.com

An incident response analyst on duty can be contacted at this email address during hours of operation.

Urgent cases can be reported by phone, +33 1-5898-7200 on a 24/7/365 basis.

4 - Charter

4.1 Mission Statement

Within Group Société Générale, the Information Security & Risks department (ISR) translates the security strategy in actionable plans, oversees the level of implemented security controls, responds to incidents and establishes operational security baseline.

CERT SG is the Group's unit in charge of incident response, digital forensics, malware analysis, and threat intelligence activities.

CERT SG's main mission is to support Société Générale Financial Group's ability to deliver on business goals while protecting it from cyberattacks that would hamper the integrity of its informational and infrastructural assets or damage its reputation. CERT SG's activities cover prevention, detection, response, containment, eradication, recovery and post-incident activities as depicted in the incident response cycle.

While delivering on objectives, CERT SG is driven by the following values:

- CERT SG strives to act in accordance with the highest standards in terms of ethics, integrity, honesty and professionalism,
- CERT SG is committed to deliver high quality services to the clients within its constituency and while responding to external parties,
- CERT SG does its best to respond to security incidents as efficiently as possible within the best possible delays,
- CERT SG facilitates information exchange between Group Société Générale entities and its peers on a need-to-know basis.

4.2 Constituency

The constituency of CERT SG is composed of all institutions and organizations belonging to the Société Générale Financial Group. Please refer to the following resource for more details:
https://www.societegenerale.com/en/content/all-groups-websites

4.3 Affiliation

CERT SG is affiliated to the Société Générale Group. CERT SG strives to maintain regular contacts with various national and international CSIRT, CERT, incident response and security teams whenever such communication follows Société Générale's needs and communication culture.

4.4 Authority

CERT SG operates under the authority of the Société Générale Group Chief Information Security Officer.

5 - Policies

5.1 Types of Incidents and Level of Support

CERT SG handles all types of incidents impacting the confidentiality, integrity or availability of Group Société Générale information systems and processes.

Depending on the incident, CERT SG's expertise may cover, but is not limited to the areas of incident response, digital forensics, malware analysis, strategical, tactical and operational threat intelligence.

CERT SG will adjust the extent of provided support depending on the incident's severity, its potential impact and the available staff resources at the time of the incident.

5.2 Co-operation, Interaction and Disclosure of Information

CERT SG considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar internal and external bodies, since such cooperative actions are likely to improve CERT SG's efficiency at solving day-to-day problems and specific incidents. The same goes for external information sharing when CERT SG's cooperation is likely to enable third-party CERTs, CSIRTs and other security teams to better perform their duties and resolve incidents.

5.3 Operations

CERT SG operates under the current French legal framework.

CERT SG is fully compliant with the latest approved version of CSIRT Code of Practice version 2.4 as featured at https://www.trusted-introducer.org/TI-CCoP.pdf

5.4 Communication and Authentication

CERT SG protects sensitive information in accordance with relevant French, European and Société Générale Group's regulations and policies for applicable jurisdictions. Specifically, CERT SG enforces the sensitivity markings defined by originators of information communicated to CERT SG ("originator control").

CERT SG also recognizes and follows the FIRST TLP (Information Sharing Traffic Light Protocol) version 1.0.

Communication security, including both encryption and authentication, is achieved by using PGP or any other agreed and tested means, depending on sensitivity and context.

6 - Services

6.1 Announcements

CERT SG provides announcements in the form of alerts and security briefings featuring threat intelligence of different sorts, which may include, but is not limited to detected vulnerabilities, new attack tools, techniques and processes as leveraged by the threat actors, indicators of compromise, and security measures needed to protect the Information Systems of Group Société Générale.

6.2 Alerts and Warnings

CERT SG disseminates information and intelligence on cyberattacks, technical disruptions, security vulnerabilities, intrusions, malware, and provides recommendations on how to tackle the resulting risk within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis.

6.3 Pre-emptive Security Controls

CERT SG performs pre-emptive security controls and offensive security missions (red teaming) 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.

6.4 Development of Security Tools

CERT SG develops security tools for its own use, to improve its services and support its activities as needed. These security tools can be used by other members of its constituency or by members of the larger CERT, CSIRT, SOC and broader information security community. Tools that CERT SG has decided to release as open source are available at https://github.com/certsocietegenerale

6.5 Intrusion Detection

CERT SG leverages tools, services and processes to detect potential intrusions.

6.6 Digital Forensics and Incident Response

CERT SG performs digital forensics activities whenever necessary, including but not limited to endpoint forensics, memory forensics, smartphone forensics, network forensics, cloud forensics, along with the malware analysis activities, which may result from identified forensic needs.

CERT SG performs incident response for its constituency. The incident response service as developed by CERT SG covers the 6 phases of the Incident Response process: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

7 - Incident Reporting Forms

CERT SG specifically designed incident reporting forms for internal needs, that have been developed to report constituency incidents to CERT SG.

To report an external incident from the outside, please provide the following details to CERT SG:

- contact details and organizational information such as person or organization's name, address and contact information,
- email address, phone number, PGP key if available,
- IP address(es), FQDN(s), and any other relevant technical element or comment,
- supporting technical elements such as logs to illustrate the issue.

Should you desire to forward any email message to CERT SG, please include all relevant email headers, bodies and attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

8 - Disclaimers

CERT SG will take all necessary precautions and apply its best competence and effort while preparing, notifying and alerting about an incident. However, CERT SG will take no responsibility for errors, omissions or damages resulting from the use of the information it provides.