ST CSIRT

RFC-2350

TLP	**[TLP: WHITE]** TLP: WHITE information may be distributed without restriction, subject to copyright controls.
Reference ST CSIRT	ST CSIRT_RFC2350
Version	1.2
Date	11/07/2022

About this document

Foreword: This document describes the ST CSIRT's services in compliance with the RFC 2350 document. RFC 2350 is an IETF Best Current Practice available at: https://www.ietf.org/rfc/rfc2350.txt

Date of Last Update

The current version of this document is November 07th, 2022.

Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism to inform of changes made to this document.

Locations where this Document May Be Found

The current version of this document is available on ST CSIRT public web site, at the following location:

https://www.st.com/content/st_com/en/csirt.html

Authenticating this Document

This document has been signed with the ST CSIRT PGP key and the signature file is available at the same location as the document itself.

ST CSIRT's public PGP key is given below.

Contact Information

Name of the Team

Short name: ST CSIRT

Full name: STMicroelectronics Cyber Security Incident Response Team

Address

STMicroelectronics

CSIRT (Cyber Security Incident Response Team)

190 avenue Célestin Coq – CS 60004

13106 Rousset

France

Time Zone

CET/CEST: Europe/Paris

Telephone Number

+33 4 42 68 66 66

Electronic Email Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CSIRT-ST, please contact us at: csirt[at]st.com

Public Keys and Encryption Information

PGP is used for functional exchanges between ST CSIRT and its Partners (incident reports, alerts, etc).

Fingerprint: CD5E C89B 476C 51EF 8B0D 456D 05DC DB83 020B 781D

The public PGP key is available at: https://www.st.com/content/dam/report-vulnerabilities/stmicroelectronics-psirt-public.zip

Team Members

The team is composed of security experts who work full-time on ST CSIRT activities.

Because of privacy concerns, we do not publish the names of our team members in public documents. Please contact us directly if you need more information.

Charter

Mission Statement

ST CSIRT is the Cyber Security Incident Response Team (CSIRT) of STMicroelectronics. Its missions are:

- Be the relay to the cyber security communities outside the Group
- Carry out a permanent watch on cyber security issues and threats that may impact the company
- Detect and react to cyber security anomalies and incidents impacting the company
- Coordinate the remediation of cyber security incidents
- Analyze incidents and threats related to cybercrime and propose action plans to reduce the risk

Sponsorship / affiliation

ST CSIRT is registered on Trusted Introducer: (https://www.trusted-introducer.org/directory/teams/st-csirt-fr.html)
ST CSIRT is applying to become a member of InterCERT-fr (https://cert.ssi.gouv.fr/csirt/intercert-fr/)

Authority

ST CSIRT acts under the authority of top management of STMicroelectronics.

Policies

Types of Incidents and Level of Support

ST CSIRT is the central point of contact regarding cyber security incidents in the company (Worldwide).

The level of support will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or services.

Co-operation, Interaction and Disclosure of Information

To accomplish its mission and perform its services, ST CSIRT regularly interacts with other organizations, such as CERT, Vendors, vulnerability Reporters, Customers, etc.

No sensitive information will be sent by ST CSIRT to another party without a prior agreement of the information owner.

ST CSIRT handles and processes information in secured physical and technical environments in accordance with the STMicroelectronics policy.

Communication and Authentication

The preferred method of communication is email. By default, all sensitive communication to ST CSIRT should be encrypted with our public PGP key detailed in Section “Contact Information”.

Services

Incident response

ST CSIRT provides following major services in the field of Incident Response:

- Detection,
- Analysis (information gathering, root cause, …),
- Alerting,
- Follow-up (involving different stakeholders),
- Reporting

Security advisories

Security advisories describe newly discovered vulnerabilities (and available solutions to fix them) for any IT solution used by STMicroelectronics. These advisories are continuously enriched with minor or major updates. The latter typically occurs when attack programs (aka “exploits”) are released.

Incident Reporting Forms

No specific form is needed to report security incidents to ST CSIRT from other parties.

Disclaimers

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