Sagemcom

RFC-2350

CSIRT-SC

SC_SSI_0242-B

Table des matières

1 Preamble

1.1 About this document

This document is Sagemcom CSIRT presentation according to RFC2350.

1.2 Release date

This version SC_SSI_0242-B is released on 29th of June, 2022.

1.3 Document availability

Document can be downloaded from Sagemcom website https://www.sagemcom.com/csirt/
Document can be received by email by sending a request to: csirt@sagemcom.com

1.4 Document identification and authentication

Title: CSIRT-SC – RFC 2350
Version: SC_SSI_0242-B
Document Date: 2022-06-29
Expiration: this document is valid until superseded by a later version

2 Contact information

2.1 Name of the team

LongName : CSIRT-Sagemcom
ShortName : CSIRT-SC

2.2 Address

Sagemcom CSIRT, Franck Bonnevialle, 250 route de l'Empereur, 92500 Rueil Malmaison, France

2.3 Email

csirt@sagemcom.com
This email is used both to report incident or to contact CSIRT-SC

2.4 Time Zone

GMT+1

2.5 Telephone number

Not Available

2.6 Facsimile number

Not Available

2.7 Internet Website

https://www.sagemcom.com/fr/sagemcom-csirt

2.8 Public keys and encryption

CSIRT-SC uses the following PGP public Key :
ID: 0x99028588872003E9
Fingerprint: 51BC5B3F84ABF12C43F477BE99028588872003E9

Key is available on following site:
https://pgp.circl.lu/
http://pgp.mit.edu/

2.9 Team members

CSIRT-SC's team leader is Franck Bonnevialle
The team consists of:

- ⇨ IT Security managers and analysts from Sagemcom IT security team (DSSI)
- ⇨ Pentester and analyst from Sagemcom Product Security Lab (SPSL)
- ⇨ With support of other Sagemcom teams involved in security (BU Security Officers, DSI SOC,…)

2.10 Operating Hours

Operation of CSIRT-SC are restricted to business hours (CET 09:00AM-06:00PM Monday to Friday), all year long excluding bank and public holidays.

3 Charter

3.1 Mission Statement

CSIRT-SC aims to prevent, investigate and coordinate any cyber-security incident and cyber-threat that may have an impact on Sagemcom Group's activities.

3.2 Constituency

CSIRT-SC drives his mission on 2 axes:

- Supports all IT system teams
- Supports all business and product teams (development, manufacturing, …)

Moreover CSIRT-SC can provide support to all Sagemcom staff and customers.

Support can be:

- General survey and
- Sensibilization and training, recommendations,…
- Vulnerability survey
- Incident management, Digital Forensic and Incident Response (DFIR)
- Cyber-crisis management.

3.3 Affiliation / Sponsoring organisation

CSIRT-SC is a private industrial CSIRT, owned, operated, and financed by Sagemcom.

3.4 Authority

CSIRT-SC is attached to Sagemcom Quality, Ethics and Risk Departement and placed under the authority of CISO.
CSIRT-SC works internally in cooperation with other Sagemcom Departments (IT, R&D, Business Units, Offshore sites, …).
CSIRT-SC cooperates externally with other CERT and CSIRT.

4 Policies

4.1 Types of Incidents and Level of Support

CSIRT-SC will process any security incident related to its mission.
CSIRT-SC level of support will be adjusted to provide adapted level of answer on any threat, vulnerability, incident analyse (assessment, impact, remediation).

CSIRT-SC will do its reasonable efforts to provide its answer within same working day during working hours or next business day.

4.2 Co-operation, Interaction and Disclosure of Information

Internal communication:
Security related information is shared within CSIRT-SC team.
By default, information is categorized as confidential and cannot be shared outside the team without authorization of CSIRT-SC manager. A specific level of confidentiality may be assigned to the security related information, on a case by case basis and subject to the applicable procedure within Sagemcom Group.
CSIRT-SC manager will provide a list of specific use cases approved by Sagemcom Group CISO for which the confidentiality level will be lower.

External communication:
By default, external communication is limited to a list of partners approved by Sagemcom Group CISO; typically, other CSIRT and CERT or security-oriented workgroups (CLUSIF, CESIN, InterCERT France).

4.3 Communication and Authentication

CSIRT-SC is the single point of contact for Sagemcom cyber-security topics, whether related to products of IT.
To contact CSIRT, please send an email to: csirt@sagemcom.com

For secured information exchange, the following PGP key can be used:
ID: 0x99028588872003E9
Fingerprint: 51BC5B3F84ABF12C43F477BE99028588872003E9

5 Services

CSIRT-SC provides services related to following aspects:

- General survey: technology, threat, product, IT, brand IP protection
- Sensibilisation, training, recommendations
- Vulnerability survey, audits, pentest
- Incident Response, forensic, crisis management

Some services are proactive, and some are reactive.

5.1 Proactive services

- Technical survey
- Threat intelligence and IoC
- Vulnerability survey, evaluation and notification
- Staff sensibilisation and training
- Recommendations
- Technical audit and pentest
- Forensic and proof protection
- Cyber exercise organisation
- Tool development
- Intrusion detection improvement
- Internal general information communication on Cyber-security
- Information sharing (CERT/CSIRT) and workshop

5.2 Reactive services

- Threat evaluation
- Vulnerability assessment and priority
- Alert analyse and support to SOC
- Incident assessment based on incident analyse (triage)
- Incident coordination (priority, traceability, notification, follow up)
- Support Incident resolution, remediation and recovery
- Single point de contact
- Support cyber-crisis management

6 Incident Reporting Forms

No reporting form has been developed to report incidents to CSIRT-SC.
To report an incident from outside Sagemcom organisation, please provide following information:

- Contact details (name/email and optionally phone number).
- Date of Incident discovery
- Incident general description
- Affected asset.
- Technical information subject to technical and legal feasibility.

Incident reporting form is sent by email to: csirt@sagemcom.com
Sensitive information can be cyphered using CSIRT-SC PGP key.

7 Disclaimer

CSIRT-SC will take all necessary precautions and apply its best competence and effort in the performance of its services. However, CSIRT-SC will take no responsibility for errors, omissions or damages resulting from the use of the information it provides. The services provided by CSIRT-SC are not designed or intended to address all matters of quality, safety, performance or condition of any product, material, services, systems or processes. CSIRT-SC and Sagemcom Broadband SAS expressly exclude all warranties, conditions and other terms implied by statute or by law (including but not limited to any implied warranties of merchantability and fitness for purpose).All intellectual property rights in any reports, document, graphs, charts, photographs or any other material (in whatever medium) produced by CSIRT-SC in the performance of its services, including all rights in concepts, ideas and inventions that may arise, shall belong to Sagemcom Broadband SAS.

END OF DOCUMENT