CERT-SE profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This document was last updated 2023-04-17.

1.2. Distribution List for Notifications

None

1.3. Locations where this Document May Be Found

The current version of this document can be found at:
https://www.cert.se/rapporter/RFC_2350_CERT-SE.pdf

2. Contact Information

2.1. Name of the Team

CERT-SE

2.2. Address

CERT-SE
MSB
651 81 Karlstad
Sweden

2.3. Time Zone

CET/CEST,
Central European Time/Central European Summer Time,
UTC+0100/UTC+0200

2.4. Telephone Number

+46 10 240 40 40

2.5. Facsimile Number

None

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

cert@cert.se

This address can be used to report all security incidents to which relate to the CERT-SE constituency.

2.8. Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication.
The current CERT-SE team-key can be found on
https://www.cert.se/cert_at_cert.se.asc.
Please use this key when you want/need to encrypt messages that you send to CERT-SE. When due, CERT-SE will sign messages using the same key.

2.9. Team Members

No information is provided in public.

2.10. Other Information

- See the CERT-SE webpages https://www.cert.se
- CERT-SE is certified by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/directory/teams/cert-se.html
- CERT-SE is a full member of FIRST, see http://www.first.org/members/teams/cert-se
- CERT-SE is a member of the Swedish CERT-forum, see https://certforum.se/index-en.html

2.11. Points of Customer Contact

Regular cases: use CERT-SE e-mail address or phone +46 10 240 40 40
Regular response hours: Monday-Friday, 8:00-16:30 (except public holidays in Sweden). We aim to respond within two business days.
Outside these hours the Duty Officer is available for incidents at +46 10 240 40 40

3. Charter

3.1. Mission Statement

The mission of CERT-SE is stated in Ordinance (2008:1002) with Instructions for the Swedish Civil Contingencies Agency (MSB). In brief the Ordinance states that CERT-SE shall:

1. Respond promptly when IT incidents occur by spreading information, and where needed work with the coordination of measures, and partake in work to remedy or mitigate the incident's consequences,

2. Cooperate with authorities that have specific tasks in the field of information security, and

3. Act as Sweden’s point of contact for equivalent services in other countries, and develop cooperation and information exchanges with them.

3.2. Constituency

CERT-SE is the National CERT of Sweden, and the constituency consists of the Swedish society, including but not limited to, Governmental authorities, Regional authorities, Municipalities, Enterprises and Companies. In addition, CERT-SE is also the Governmental CERT of Sweden and have additional responsibilities within the Governmental body.

3.3. Sponsorship and/or Affiliation

CERT-SE is part of MSB – The Swedish Civil Contingencies Agency, which is a Swedish governmental agency. CERT-SE is fully financed by MSB.

3.4. Authority

CERT-SE coordinates security incidents on behalf of its constituency and has no authority reaching further than that. CERT-SE is however expected to make operational recommendations regarding vulnerabilities and mitigation of incidents and/or incident handling. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such-recommendations is not a responsibility of CERT-SE, but solely of those to whom such recommendations are made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority. CERT-SE itself is the authority that can set and reset the emergency-label. An incident can be reported to CERT-SE as emergency, but it is up to CERT-SE to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information related to incidents is handled confidentially by CERT-SE, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

CERT-SE supports the Traffic Light Protocol (TLP – see https://www.first.org/tlp) - information that comes in with the tags TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT or TLP:RED will be handled appropriately.

CERT-SE will use the information you provide to help solve security incidents. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know basis, and preferably in an anonymized fashion.

If you object to this default behaviour of CERT-SE, please make explicit what CERT-SE can do with the information you provide. CERT-SE will adhere to your policy, but will also point out to you if that means that CERT-SE cannot act on the information provided.

As of October 1, 2022, on behalf of the government, MSB forwards the notifications and completed forms that are reported to MSB (regulation (2022:524), law (2018:1174) and regulation (2018:1175)), and which contain descriptions of incidents that can be assumed to have their basis in a criminal act, to the Police Authority.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP/GnuPG, or other pre-approved cryptographically means, in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

CERT-SE is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). CERT-SE therefore handles both the triage and coordination aspects. Incident resolution is left at the discretion of the involved constituents – however CERT-SE will offer support and advice on request.

5.2. Proactive Activities

CERT-SE pro-actively advises their constituency in regard to recent vulnerabilities and on matters of computer and network security.

CERT-SE is not responsible for implementation, which is always left at the discretion of the constituents.

6. Incident reporting Forms

Preferably, report in plain text using email - or use the phone.

Those cases where there is a mandate for reporting use mandating recommended means.

7. Disclaimers

None.