RFC 2350

1. About this document

1.1. Date of last update

This is version 1.1, published on 1st January 2014.

1.2. Distribution list for notifications

Currently CSUC-CSIRT does not use any distribution lists to notify about changes in this document.

1.3. Locations where this document may be found

The current version of this CSIRT description document is available from the CSUC web site; its URL is http://www.csuc.cat/en/communications/security/incident-response-team. Please make sure you are using the latest version.

1.4. Authenticating this document

This document has been signed with the CSUC-CSIRT PGP key. The signature is also on our web site, under: http://www.csuc.cat/content/claus-pgp-publiques

2. Contact information

2.1. Name of the team

CSUC-CSIRT: Equip de Resposta a Incidents de l'Anella Científica.

2.2. Address

CSUC-CSIRT: Equip de Resposta a Incidents de l'Anella Científica.
Centre de Supercomputació de Catalunya
C/ Gran Capità 2-4 (Edifici Nexus)
08034 Barcelona

2.3. Time zone

Central European Time (GMT+0100, Brussels, Copenhagen, Madrid, Paris)

2.4. Telephone number

+34 932056464

2.5. Facsimile number

None available.

2.6. Other telecommunication

None available.

2.7. Electronic mail address

Incident reports (including non-incident) related mail should be addressed to <eriac (at) csuc cat>

2.8. Public keys and other encryption information

CSUC-CSIRT has an OpenPGP public key, which KeyID is 0x5EDAFA81 and fingerprint is: BCE7 7D8E 172B FA9C AF77 B17A A2F2 23EB 5EDA FA81

The public key and its signatures can be found at the usual large public keyservers, or on CSUC's web site, under: http://www.csuc.cat/content/claus-pgp-publiques

Each CSUC-CSIRT team member has also a respective OpenPGP public key that you can fetch from the CSUC's website.

2.9. Team members

CSUC-CSIRT is the “Equip de Resposta a Incidents de l'Anella Científica” . CSUC-CSIRT is operated by CSUC (Centre de Supercomputació de Catalunya) and the Anella Científica is the high-speed communications network, created by the Fundació Catalana per a la Recerca i la Innovació in 1993 and managed by CSUC, that connects universities and research centers in Catalunya. The Anella Científica provides a wide data transmission capacity among all the connected institutions so that information exchange is facilitated connections to RedIRIS' research networks and the ones connected to that one are improved, and the use and the development of broadband applications are fostered.

2.10. Other information

Any other informations about CSUC-CSIRT, can be found at http://www.csuc.cat

2.11. Points of customer contact

The preferred method for contacting CSUC-CSIRT is via e-mail at <eriac (at) csuc cat>. We encourage our constituency (customers) to use PGP encryption when sending any sensitive information to CSUC-CSIRT.

If it is not possible (or not advisable for security reasons) to use e-mail, CSUC-CSIRT can be reached by telephone during regular office hours.

CSUC-CSIRT hours of operation are restricted to: 09:00-18h00 CET Monday to Friday.

3. Charter

3.1. Mission statement

CSUC-CSIRT is aimed to the early detection of security incidents affecting centers affiliated to the Anella Científica, as well as the coordination of incident handling with them. Proactive measures are in constant development, involving timely warning of potential problems, technical advice, training and related services.

3.2. Constituency

CSUC-CSIRT offers full service (incident handling and coordination with other IRTs as a last point of contact for emergency or high priority security matters) to all organizations conneceted to Anella Científica.

3.3. Sponsorship and/or Affiliation

CSUC-CSIRT is sponsored by CSUC (Consorci de Serveis Universitaris de Catalunya). CSUC provides advanced communication services to the scientific community and national universities.

3.4. Authority

CSUC-CSIRT operates under the auspices of, and with authority delegated by, the director of CSUC.

CSUC-CSIRT expects to work cooperatively with system administrators and users at Anella Científica connected institutions, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, CSUC-CSIRT has the authority to take the measures it deems appropriate to properly handle a computer security related incident.

4. Policies

4.1. Types of incidents and level of support

CSUC-CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, in the constituency networks. CSUC-CSIRT may act upon request of one of its constituents, or may act if a constituent is, or threatens to be, involved in a computer security incident.

The level of support given by CSUC-CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CSUC-CSIRT's resources at the time, though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity and extent.

End users are expected to contact their systems administrator, network administrator, or department head for assistance.

4.2. Co-operation, interaction and disclosure of information

CSUC-CSIRT exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. No personal nor overhead data are exchanged unless explicitly authorized.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are encrypted if they must be transmitted over unsecured environment as stated below.

4.3. Communication and authentication

In view of the types of information that CSUC-CSIRT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the CSUC-CSIRT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within the constituency, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

CSUC-CSIRT keys can be found in http://www.csuc.cat/content/claus-pgp-publiques

5. Services

5.1. Incident response

CSUC-CSIRT will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management:

5.1.1. Incident triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2. Incident coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3. Incident resolution

- Helping to remove the vulnerability.

- Helping to secure the system from the effects of the incident.
- Collecting evidence of the incident.

In addition, CSUC-CSIRT will collect statistics concerning incidents processed, and will notify the community as necessary to assist it in protecting against known attacks.

5.2. Proactive services

CSUC-CSIRT coordinates and maintains the following services to the extent possible depending in its resources:

- CSUC-CSIRT tries to raise security awareness in its constituency.
- Collect contact information of local security teams.
- Publish announcements concerning serious security threats.
- Observer current trends in technology and distribute relevant knowledge to the constituency.
- Provide fora for community building and information exchange within the constituency.

6. Incident reporting forms

CSUC-CSIRT has created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out. The current version of the form is available from: http://www.csuc.cat/content/reportar-un-incident

7. Disclaimers

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