CERT-CS CSIRT RFC2350 profile

1. DOCUMENT INFORMATION

1.1. DATE OF LAST UPDATE

This is version 1.00, published 2015/02/05.

1.2. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CSIRT description document is available from the CERT-CS intranet site at the following URL : http://portail.seducs/projects/bu-defense/files/), or from the CERT public website at the following URL : http://www.c-s.fr/attachment/588734/.
Please make sure you are using the latest version.

1.3. AUTHENTICATING THIS DOCUMENT

This document has been signed with the CERT-CS PGP key. The signatures are available on our intranet site at the following URL : http://portail.seducs/projects/bu-defense/files/, or on the public website at the following URL : http://www.c-s.fr/attachment/588717/.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

"CERT-CS": the CS Systèmes d'Information Computer Emergency Response Team.

2.2. ADDRESS

CS Systèmes d'Information
22, avenue Galilée
92350 Le PLESSIS-ROBINSON
France

2.3. TIME ZONE

Europe/Paris (CET/GMT+1 from october to march, CEST/GMT+2 from april to september).

2.4. TELEPHONE NUMBER

(+33) 1 41 28 94 48

2.5. FACSIMILE NUMBER

(+33) 1 41 28 42 84

2.6. OTHER TELECOMMUNICATION

None available.

2.7. ELECTRONIC MAIL ADDRESS

<cert-cs@c-s.fr> This is a mail alias that relays mail to CERT-CS team members.

2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

The CERT-CS has a PGP key, whose KeyID is 0EA14CFF and whose fingerprint is :
D1 A7 9E 77 99 9E 56 AD 5E DB DC 31 CA D1 02 6D 0E A1 4C FF.
The CERT-CS CSIRT coordinator can confirm by telephone or in person CERT-CS's PGP key fingerprint to customers or fellow CSIRT coordinators.

CERT-CS ASCII-Armored public PGP key is :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQINBFTTF0MBEACekDxQIgNIl2mE+p+BjIitxWQ8fNzMNDj/xTkXNwDNNwY9qaya
yUwghUVAVEINnD5vmziLVqKMWs/S8hhMZCKyPmwikPPMx4cTPNytrm4Bm+3P2zV5
4TAqIzRkKPMGqTBae+MwkCRiVQTpWIlFtCrL4rTu2YzTD2J4l3y0lpTPrZn+umt0
DY73unyN1TBepLjbf+vis+nZfK7MjoovCfktODu30BMAXw8oNidtheUrv6+S4Yn2
yPTUqyY6QDB57wp/fTYAcStymQEpnTdk5GNmW+pp7cedvw2XlqCMQLKC/oPSlh19
Uh9Rq97Q9Q4vcH9cjG/TtAFhWo99iGmn9lwT/epyDP9dcFaPi8YbaAx9cHE38g5V
Z10LomBI7NBSByqLBl+/MV63XMbBC9EbZ1Ym6zooCoQtEwVOMYCMb254sOR+og0R
JGfjSzm+7xadojC4bhbysG7kjjgUYFsz9uvpFWkrWmY1JLVGx+yBfLLOaROqB0+e
pdaT7Kfw9uq98lGh2p5VMETgyq9ZHaQPZKshbtYvRQa3XL2JdyB6UUI0xD2bW+J0
EaoYSRZK4DHgyEIuDAwWgGabch1DMK8+v1sJwscgHIMLPsJId/qqGIIgh9QDN+cC
GxGeHOvzwT6RP7QstntIhYOsb8iTNhuE33a00vBszU5U+VaIZJTdqmdaVQARAQAB
tB5DUy1DRVJUIENTSVJUIDxjZXJ0LmNzQGMtcy5mcj6JAj8EEwECACkFAlTTF0MC
Gw8FCQPD7m0HCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRDK0QJtDqFM/zh/
D/wJ0nBRw+3i1xxtKw9aXavnDyQizifAulHVS/yYrLvqktZ8M/za0+IzZByP55uF
GsnWI1sg2pdRwP9l5uprzYXkvh6JY9Bg/DKwcd06NsmrGgwBtiEVref/t63WVfhJ
UkMZwHelTveH3gdA0GnqpNM3nHoM9/bdFH6NLnoF3m3NqZxf+EHrgJNTxc6aE/S9
XkV+izPltYsgeg/pOOSB3B9/O1mQfviwOOCb95bTeNet0ngGhcPdgeemhkDiPvqA
F1p6iJSieKrL6QLQjTcIGlIdJrz1SDtLG4VLb4GXXI5xF1jFQS3pgPkKdZhGt6DK
TNO6Y/UMEGfF2ae/7RXT+yjgNA+mkdSICN7At6EVuqiz7PuBkEM1B695YGerC5hP
D8uq4YXH8S8W4uZhrSwFd/iFA6Rz2DXtgSQ3tEe/LWl/gpif9okOyQ+qlMV1UBBi
p05tnAfBxRFMnfp7G2IDniY5EIuJqFQBztZyXbaHbq44fCNppYWKKWXOrCE9m0Tn
1/Ty15/SezIAh8wh7Bjc6ouu/8I1G3NsbYTNkYCMCg0efgsX1q+agfCMQkH/2Nmn
cFugO8OsRve9WnXUsYfsD6uz+2fYMgCG1whRvaapB4w9uq3KPxYmxGOniyGc0ksG
2vy/O9/IDoWJtKH6Cu6iAq51RgBLNAerRFK/1fx4N+Qn+w==
=gyLI
-----END PGP PUBLIC KEY BLOCK-----
```

2.9. TEAM MEMBERS

Thomas Brethomé of CSSI's Defence, Security & ATM (DSA) Business Unit is the CERT-CS coordinator.
Jean-Yves Faye of CSSI's DSA Business Unit is the CERT-CS backup coordinator.
Management and liaison is provided by Patrice Bouf, program manager, CSSI.

2.10. POINTS OF CUSTOMER CONTACT

The preferred method for contacting the CERT-CS is via e-mail at <cert.cs@c-s.fr>; e-mail sent to this address will be automatically forwarded to the CERT-CS CSIRT team, immediately. If you require urgent assistance, put "urgent" in your subject line.
If it is not possible (or not advisable for security reasons) to use e-mail, the CERT-CS can be reached by telephone during regular office hours.
The CERT-CS's hours of operation are generally restricted to regular business hours (08:00-16:00 Monday to Friday except holidays).

3. CHARTER

3.1. MISSION STATEMENT

The purpose of the CERT-CS is, first, to provide vulnerability analysis, patch management and other proactive mesures to existing projects developped by CSSI, and second, to assist CSSI projects and services in responding to security incidents when they occur.

3.2. CONSTITUENCY

CERT-CS's constituency is CSSI's projects using the SEDUCS operating system. CERT-CS may provide CERT support to other public or private organizations upon signing a binding legal agreement.

3.3. SPONSORSHIP AND/OR AFFILIATION

CERT-CS is part of CSSI's Defence, Security & ATM Business Unit.

3.4. AUTHORITY

CERT-CS coordinates security incidents on behalf of its constituency. CERT-CS is however expected to make operational recommendations regarding vulnerabilities and mitigation of incidents and/or incident handling. The implementation of such recommendations is not a responsibility of CERT-CS, 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-CS itself is the authority that can set and reset the EMERGENCY status. An incident can be reported to CERT-CS as EMERGENCY, but it is up to CERT-CS 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-CS, 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 or vulnerability 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-CS will use the information you provide to help solve security incidents and/or vunlnerability, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymized fashion.

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

CERT-CS does not report incidents to law enforcement, unless national law requires so. Likewise, CERT-CS only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that CERT-CS

cooperates in an investigation. When a court order is absent, CERT-CS will only provide information on a need-to-know base.

4.3. COMMUNICATION AND AUTHENTICATION

See 2.8 above. Usage of PGP/GnuPG, or other pre-approved cryptographical means, in all cases where sensitive information is involved is highly recommended.
In cases where there is doubt about the authenticity of information or its source, CERT-CS reserves the right to authenticate this by any (legal) means.

5. SERVICES

5.1. INCIDENT RESPONSE

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

5.2. PROACTIVE ACTIVITIES

CERT-CS pro-actively advises their constituency in regard to recent vulnerabilities and on matters of computer and network security. CERT-CS is not responsible for implementation, that is always left at the discretion of the constituents.

6. INCIDENT REPORTING FORMS

Not available. Preferably report in plain text using e-mail - or use the phone.

7. DISCLAIMERS

None available.