EGI CSIRT - RFC 2350

EGI-CSIRT profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version 0.10 of 01. Jul. 2020.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 .

E-mail notification of updates are sent to:

• All EGI-CSIRT members

• All EGI-CSIRT constituents

Any questions about updates please address to the EGI-CSIRT e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on https://confluence.egi.eu/display/EGIBG/EGI+CSIRT+-+RFC+2350.

2. Contact Information

2.1. Name of the Team

Full name: EGI-CSIRT

Short name: EGI-CSIRT

EGI-CSIRT is the CERT or CSIRT team for EGI (http://www.egi.eu/about/EGI.eu/), A research-or-educational / non-commercial-organisation in The Netherlands.

2.2. Address

EGI.eu

Science Park 140

1098 XG Amsterdam, NL

The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

Regular telephone number: +31 (0)20 89 32 007 (EGI.eu secretary telephone number)

Emergency telephone number +31 (0) 630 372 691 (EGI.eu Director)

2.5. Facsimile Number

No-Fax-Number

2.6. Other Telecommunication

```
email: contact@egi.eu
```

2.7. Electronic Mail Address

abuse@egi.eu

This address can be used to report all security incidents to which relate to the EGI-CSIRT constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication.

The current EGI-CSIRT team-key can be found on

https://wiki.egi.eu/wiki/EGI_CSIRT:PGP

and is also present on the public key servers.

Please use this key when you want/need to encrypt messages that you send to EGI-CSIRT. When due, EGI-CSIRT will sign messages using the same key.

When due, sign your messages using your own key please - it helps when that key is verifiable using the public key servers.

2.9. Team Members

No information is provided about the EGI-CSIRT team members in public.

2.10. Other Information

See the EGI-CSIRT webpages https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page and https://csirt.egi.eu/

2.11. Points of Customer Contact

Regular cases: use EGI-CSIRT e-mail address.

Regular response hours: Monday-Friday, 09:00-17:00 (except public holidays (Christmas, New Years eve, Easter)).

EMERGENCY cases: send e-mail with EMERGENCY in the subject line.

3. Charter

3.1. Mission Statement

The mission of EGI-CSIRTis to co-ordinate the resolution of IT security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring.

3.2. Constituency

The constituency for EGI-CSIRTis EGI.eu (http://www.egi.eu/about/EGI.eu/) A research-or-educational /not-for-profit foundation established under Dutch law in The Netherlands. This constituency consists of: An overview of the 50+ above mentioned integrated RPs/ participating countries and resource centers are in: https://www.egi.eu/federation/data-centres/

3.3. Sponsorship and/or Affiliation

EGI-CSIRTis part of Egi.eu, is a not-for-profit foundation established under Dutch law to coordinate and manage the European Grid Infrastructure (EGI) federation on behalf of its participants: National Grid Initiatives (NGIs) and European International Research Organisations (EIROS).

3.4. Authority

The team coordinates security incidents on behalf of their constituency and has the authority to remove Resource Centers from its infrastructure (EGI). The team is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to remove Resource Centers from its infrastructure (EGI). The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. EGI-CSIRT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to EGI-CSIRT as EMERGENCY, but it is up to EGI-CSIRT to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by EGI-CSIRT, 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.

EGI-CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP – see hhttps://www.trusted-introducer.org/ISTLPv11.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

EGI-CSIRT will use the information you provide to help solve security incidents, 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 anonymised fashion.

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

EGI-CSIRT does not report incidents to law enforcement, unless national law requires so. Likewise, EGI-CSIRT 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 EGI-CSIRT cooperates in an investigation. When a court order is absent, EGI-CSIRT will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP/GnuPG in all cases where highly sensitive information is involved is highly recommended.

In cases where there is doubt about the authenticity of information or its source, EGI-CSIRT reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

EGI-CSIRT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). EGI-CSIRT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however EGI-CSIRT will offer support and advice on request.

5.2. Proactive Activities

EGI-CSIRT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking /cracking. EGI-CSIRT advises Egi.eu on matters of computer and network security. It can do so pro-actively in urgent cases, or on request. Both roles are roles of consultancy: EGI-CSIRT is not responsible for implementation.

6. Incident reporting Forms

https://confluence.egi.eu/display/EGIBG/Incident+reporting

7. Disclaimers

This is the 1.1 version of EGI-CSIRT's rfc-2350