CSIRT Description for CERT Energa

==========

1. About this document

1.1 Date of Last Update

This is version 1.0, published on 22 July 2019.

1.2 Distribution List for Notifications

Currently CERT Energa 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 CERT Energa WWW site; its URL is https://cert.energa.pl/kontakt
Please make sure you are using the latest version.

2. Contact Information

2.1 Short Name of the Team

CERT Energa

2.2 Name of the Team

Computer Emergency Response Team Energa

2.3 Address

CERT Energa

Energa Informatyka i Technologie sp. z o.o.

Aleja Grunwaldzka 472A

80-309 Gdańsk

Poland

2.4 Time Zone

Central European Time (GMT+0100, GMT+0200 from April to October)

2.5 Telephone Number

landline: +48 58 527 91 11

2.6 Facsimile Number

None available at this moment

2.7 Electronic Mail Address

cert@energa.pl

2.8 Public keys and Other Encryption Information

Not available at this time

2.9 Other Information

General information about CERT Energa, as well as links to various recommended security resources, can be found

at https://cert.energa.pl/

2.10 Points of Customer Contact

The preferred method for contacting CERT Energa is via e-mail at <cert@energa.pl>;

e-mail sent to this address will be handled by the responsible human.

If it is not possible (or not advisable for security
reasons) to use e-mail, CERT Energa can be reached by
telephone 24/7.

CERT Energa hours of operation are generally restricted
to regular business hours (08:00 - 16:00 CET/CEST Monday
to Friday except holidays) with 24/7 on-call duty service.

3. Charter

3.1 Mission Statement

The main role of CERT Energa is the operational service of global ICT
security incidents with early warning, threat detection, malware analysis,
issuing security messages, security assessments and audits as well
as consultations in the field of IT security.

3.2 Constituency

CERT Energa constituency is:

- ASN: 28689

- IP: 91.208.150.0/24 and 91.209.155.0/24;

- Domains: actaenergetica.org,cieplokaliskie.com.pl, e-elektrownie.pl, elektrowniaostroleka.pl, energa-finance.se, energa-kogeneracja.pl, energa-operator.pl

energa-slovakia.sk, energa.pl, energaathleticcup.pl, energabasketcup.pl, energasailing.pl, energasport.pl, energawisla.pl, partnerenerga.pl, planetaenergii.pl

salonenerga.pl, swiecsie.pl

3.3 Sponsorship and/or Affiliation

CERT Energa is financially maintained by the Grupa Energa which it is formally a part of.

3.4 Authority

Authority The CERT Energa operates under the auspices of, and with authority delegated by Energa S.A.

The CERT Energa expects to work cooperatively with system administrators and users (customers) at Grupa Energa network

However, should circumstances warrant it, the CERT Energa 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

CERT Energa is authorized to address all types of

computer security incidents which occur, or threaten to

occur, in Grupa Energa networks.

The level of support given by CERT Energa 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 the CERT Energa resources at the time.

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

4.2 Co-operation, Interaction and Disclosure of Information

CERT Energa 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 sensitive 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

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, GPG 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.

5. Services

5.1 Incident Response

CERT Energa will assist system administrators in handling the technical and organizational aspects of the 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

CERT Energa will give advice but no physical support whatsoever to customers from the Grupa Energa internal network with respect to the incident resolution.

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Collecting the evidence of the incident.

In addition, CERT Energa 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

CERT Energa coordinates and maintains the following services to the extent possible depending on its resources:

- Information services through the following channels:
    - website: https://cert.energa.pl/
- Training and educational services

6. Incident Reporting Forms

CERT Energa only handles incidents reported by e-mail or phone. Contact data is available at: https://cert.energa.pl/kontakt/

7. Disclaimers

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