GRNET-CERT Profile

1 Document Information

This document describes GRNET-CERT according to RFC 2350.

1.1 Date of Last Update

This is version 1.2.0, published December 11, 2019.

1.2 Distribution List for Notifications

The latest version of this profile can be found on the location specified in 1.3 .

1.3 Locations where this Document May Be Found

The current version of this document is available from the GRNET CERT website located at https://cert.grnet.gr .

1.4 Authenticating this Document

There is no available mean for authentication of this document.

1.5 Document Identification

Title:	"RFC 2350 – GRNET-CERT"
Version:	1.2.0
Document Date:	December 11, 2019
Expiration:	This document is considered valid until superseded by a later version.

2 Contact Information

2.1 Name of the Team

GRNET-CERT is the Computer Emergency Response Team for the National Infrastructures for Research and Technology. Short name: GRNET-CERT

2.2 Address

GRNET-CERT
Kifisias 7 11523 Athens,
Greece

2.3 Time Zone

GMT+02/GMT+03

2.4 Telephone Number

+30 210 7474401

2.5 Facsimile Number

+30 210 7474490

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

Please send incident reports at grnet-cert@grnet.gr and cert@grnet.gr.

2.8 Public Keys and Other Encryption Information

User ID: GRNET CERT cert@grnet.gr
Fingerprint: AB282D0F01688D2938E5470AEF9BCF8F79CD0710
Key type: rsa4096 Expires: 2023-11-10

2.9 Team Members

Dimitris Mitropoulos	dimitro@grnet.gr
Eirini Degkleri	degleri@noc.grnet.gr
Thanos Giannopoulos	thanosgn@noc.grnet.gr

2.10 Other Information

GRNET-CERT is accredited by the Trusted Introducer for CERTs in Europe. More information at `https://www.trusted-introducer.org/directory/teams/grnet-cert.html`

2.11 Points of Customer Contact

The preferred method for contacting GRNET-CERT is via e-mail at: grnet-cert@grnet.gr If it is not possible (or not advisable for security reasons) to use e-mail, GRNET-CERT can be reached by telephone during business hours: 09:00 to 17:00 Monday to Friday.

3 Charter

3.1 Mission statement

GRNET-CERT provides incident response and security services to both the National Infrastructures for Research and Technology (GRNET) and to all Greek Universities, research institutes and educational networks in Greece.

3.2 Constituency

The constituency of GRNET-CERT refers to the network services provided by National Infrastructures for Research and Technology (GRNET), that is, the Greek universities, research institutes, educational organizations and government agencies. The list of ASNs, Domains, IP ranges is described here:
5408
62.217.80.0/20
62.217.96.0/19
83.212.0.0/21
83.212.72.0/21
83.212.80.0/21
83.212.96.0/19
83.212.168.0/21
194.177.208.0/22
195.130.123.0/24
195.251.24.0/22
195.251.62.0/24

3.3 Sponsorship and/or affiliation

GRNET-CERT serves the Greek Research and Technology Network `https://grnet.gr/en/` . GRNET is present in global networking for research and education, representing Greece in GÉANT.

3.4 Authority

The activities of GRNET-CERT encompass a fairly wide area of interests and activities in the computer security field.

4 Policies

4.1 Types of incidents and level of support

GRNET- CERT is committed to informing its constituency and to issue alerts and warnings. Furthermore, it analyzes the logs from incidents, vulnerabilities and artifacts and performs incident response and security forensics. The team actively maintains and tests a list of updated security software tools that are used to assist in various activities such as system audits, vulnerability analysis, antivirus and malware handling tasks. These tools are available to all interested parties and to the best of the teams knowledge do not contain software that may exploit known or unknown system vulnerabilities. In addition, it collects various documents related to security issues, such as technical "how to" guides and documentation on system security related techniques, such as system installations, evidence handing, etc.

4.2 Co-operation, interaction and disclosure of information

The team participates in the TF-CSIRT (Task Force - Computer Security Incident Response Team) program of TERENA and when possible, attends its regular quarterly meetings. It also participates in the Trusted Introducer initiative of TERENA that has been established to facilitate the communication between European CSIRTs. GRNET-CERT received its accreditation in April 2003.

Also, the incident handling process includes both the incident analysis and the response coordination to other CERTs. To this end GRNET-CERT is a member of *CERTCOOP:Trans-European and Greek CERTs collaboration project.*

4.3 Communication and authentication

For normal communication not containing sensitive information GRNET-CERT might use conventional methods like unencrypted e-mail or fax. For secure communication PGP-encryption is also available. The GRNET-CERT PGP public key is mentioned at section 2.8.

5 Services

5.1 Incident response

GRNET-CERT will inform and assist IT-security teams and NOCs in handling and responding to incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident triage

- Investigating the validity of the incident
- Determining the operational impact of the incident
- Assigning a priority for incident response

5.1.2 Incident coordination

GRNET-CERT coordinates with IT-security teams and more specific CERTs in Greece. The main activity of the team is the effective response to security incidents involving its constituency. This is accomplished by acting as an intermediary between affected parties and offering, when required, technical advice leading to the resolution of the incident. The affected parties may be internal or external entities to GRNET. Incidents are recorded, analyzed and monitored until they are considered resolved. In cases that legal concerns arise from security incidents, the team offers its services in coordination with legal representatives of GRNET following to the established Greek laws regarding privacy and handling of electronic evidence and communication.

5.1.3 Incident resolution

Incidents are recorded, analyzed and monitored until they are considered resolved. In cases that legal concerns arise from security incidents, the team offers its services in coordination with legal representatives of GRNET following to the established Greek laws regarding privacy and handling of electronic evidence and communication.

5.2 Proactive activities

The proactive services of GRNET-CERT include:

- security announcements
- technology watch
- security audits and assessments
- development of security tools
- intrusion detection systems

Also, it coordinates with other Greek CERTs to exchange information and to raise security awareness in its constituency.

6 Incident reporting forms

Available on the website of GRNET-CERT.

7 Disclaimers

None.