2019-02-20

GÉANT CERT RFC2350 Description

Date:	2019-02-20
Dissemination Level:	Public
Owner:	COO
Authors:	GÉANT

Document Revision History

Version	Date	Description of change	Person/Position
1.0	2014-10-10	First version issued	Jan Kohlrausch – Security Officer
1.1	2015-03-17	Update CERT and company name	Evangelos Spatharas – Security Engineer
1.2	2015-05-10	Update Company logo	Evangelos Spatharas – Security Engineer
1.3	2016-02-10	Revision of Constituency	Fotis Gagadis – Security Officer Evangelos Spatharas – Security Engineer
1.4	2017-06-28	Revision of Constituency	Fotis Gagadis – Security Officer
1.5	2018-04-17	Update on 2.9 section and revision of the RFC	Evangelos Spatharas – Head of Security
1.6	2019-02-20	Contacts update	Evangelos Spatharas – Head of Security

Table of Contents

1 DOCUMENT INFORMATION

1.1 DATE OF LAST UPDATE

2019-02-20

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

Not Applicable

2 CONTACT INFORMATION

2.1 NAME OF THE TEAM

Official name:

GÉANT Computer Emergency Response Team (CERT)

Short name:

GÉANT CERT

2.2 ADDRESS

GÉANT CERT
City House
126-130 Hills Road
Cambridge
CB2 1PQ, UK

2.3 TIME ZONE

Time zone is UTC

2.4 TELEPHONE NUMBER

Main number:

+44 1223 733033

2.5 FACSIMILE NUMBER

Left intentionally blank

2.6 OTHER TELECOMMUNICATION

Not applicable

2.7 ELECTRONIC MAIL ADDRESS

Please send incident reports which relate to the GÉANT Project or GÉANT Association network to cert@oc.geant.net.

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

```
User ID:      GÉANT CERT <cert@oc.geant.net>
Key ID:       0x99833085       Key type:      RSA
Key size:     4096             Expires:       never
Fingerprint:  3CBF F211 8305 635D 5839  BB27 BA6B F34A 9983 3085
```

2.9 TEAM MEMBERS

The CÉANT CERT team is made up of security experts from within GÉANT Association working on departments that have direct impact on GÉANT operations and Project. The team consists of people from the following departments:

- OC department
- NE department
- Information Technology department
- Security department
- SWD department

2.10 OTHER INFORMATION

Other information is available at the Trusted Introducer directory at

https://www.trusted-introducer.org/directory/teams/geant-cert.html

Or through GÉANT website

https://www.geant.org/Networks/Network_Operations/Network_Security/Pages/GEANT_CERT.aspx

2.11 Points of Customer Contact

The preferred method for contacting is via e-mail:

- For security incidents to cert@oc.geant.net

3 Charter

3.1 Mission Statement

GÉANT CERT is the Computer Emergency Response Team (CERT) of GÉANT serving users of services delivered by GÉANT. The main constituents are National Research and Education Networks (NRENs) in the GÉANT Project. It deals with computer and network security incidents related to DDOS, Bots, Spamming and infrastructure vulnerabilities that involve services operated by GÉANT Association- for example the GÉANT Project network.

3.2 Constituency

The primary constituency are NRENs and associated CERTs participating in the GÈANT Project and/or connected to the GÉANT Project network.

3.3 Sponsorship and/or Affiliation

GÉANT Association was established in 1993 to coordinate pan-European research and education (R&E) networking on behalf of Europe's National Research and Education Networks (NRENs).

GÉANT Project, the flagship project, serves approximately 50 million users across Europe, reaches over 100 countries worldwide and its one of the most advanced international networks of its type. Like many of our projects it is co-funded by the European Commission along with European NRENs.

3.4 Authority

The GÉANT CERT operates under the auspices of, and with authority delegated by, the GÉANT Association.

GÉANT CERT assists NRENs and associated CSIRTs to analyse, resolve, and to mitigate network based attacks. As such, it provides services to detect anomalies and attacks on the backbone and to apply network filter to mitigate distributed denial of service attacks.

4 POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

GÉANT CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, on GÉANT Association or GÉANT Project network. These include, for example, distributed denial of service attacks, network scans, and compromised machines.

The level of support given by GÉANT Association 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 GÉANT CERT's resources at the time. Resources will be assigned according to the following priorities, listed in decreasing order:

- Incident affecting the confidentiality and integrity of data or systems in GÉANT Association or GÉANT Project network;
- Incidents that seriously affect the operation and availability of the GÈANT Project network;
- Incidents that affect the NREN networks (e.g. distributed denial of service attacks);
- All other attacks that affect the NREN networks.

GÉANT CERT **assists the NRENs to mitigate or to resolve from these incidents** which includes, for example, to block malicious traffic. Furthermore, the NRENs are informed about security incident that have been detected on the GÈANT Project network and are related to their network.

Note that **no direct support will be given to end users;** they are expected to contact their system administrator, network administrator, or department head for assistance. The GÉANT CERT will support the latter people.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

GÉANT CERT strives to closely collaborate with the NREN and CSIRT community to protect the infrastructure and data of the GÉANT Project.

If not agreed otherwise, supplied information are kept confidential. Only data that is required to resolve from the specific incident are disclosed to concerned parties (need to know). GÉANT CERT provides means to support confidentiality and integrity of data that is submitted to or disclosed by GÉANT CERT.

For data classification, GÉANT CERT supports the Information Sharing Traffic Light Protocol that comes in with the tags WHITE, GREEN, AMBER or RED. **All incident reports will be tagged as AMBER by default unless otherwise stated**. A description can be found at:

https://www.trusted-introducer.org/ISTLPv11.pdf

4.3 Communication and Authentication

GÉANT CERT supports PGP for encrypted mails whereas the usage of PGP in all cases where sensitive information is involved is highly recommended. The details of the current PGP key can be found in Sec. 2.8.

Requests for information or security controls such as firewall filters are restricted to authorised NREN or associated CSIRT members. For authentication issues, GÉANT maintains information about authorised representatives or use other means (e.g. telephone call back) to authenticate a person.

5 Services

5.1 Incident Response

GÉANT CERT will assist system administrators and NREN CSIRTs in handling the technical and organizational aspects of security incidents on the GÈANT Project and GÉANT Association network only. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.2 Incident Triage

- Assessment of the severity of the incident. If required the incident will be escalated to the General Management;
- Hand off to the appropriate team (e.g. GÉANT Operations Centre).

5.3 Incident Coordination

- Determining the cause and extend of the incident and involved sites (e.g. DDoS);
- Dissemination of incident reports to NRENs.

5.4 Incident Resolution

- Providing advice to affected sites;
- Removing the vulnerability;
- Securing the system from the effects of the incident;
- Application of network filters, if applicable.

5.5 Proactive Activities

- Network monitoring to detect attacks as early as possible;
- Sharing information with the CSIRT community and constituency.

6 Incident Reporting Forms

There are no reporting forms available.

7 Disclaimers

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