საქართველოს იუსტიციის სამინისტრო

მონაცემთა გაცვლის სააგენტო

RFC 2350

CSIRT Description for CERT-GOV-GE

1. About this document

1.1 Date of Last Update

This is version 1.01, published 20 April , 2012.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list <certusers@cert.gov.ge>. Subscription requests for this list should be sent to the Majordomo at <cert@cert.gov.ge>; the body of the message should consist of the word "subscribe". Send the word "help" instead if you don't know how to use a Majordomo list manager.

This mailing list is moderated.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the CERT-GOV-GE WWW site; its URL is http://www.cert.gov.ge/rfc2350.txt Please make sure you are using the latest version.

2. Contact Information

2.1 Name of the Team

"CERT-GOV-GE": the Computer Emergency Response Team Government Georgia.

2.2 Address

CERT Government Georgia

Ministry Of justice Of Georgia

LEPL Data exchange Agency - DEA

2, St. Nicholoz/N. Chkheidze Str.,

0102, Tbilisi

Georgia

2.3 Time Zone

Georgia Standard Time (UTC/GMT +4 hours)

2.4 Telephone Number

+995 32 2915140 (ask for CERT-GOV-GE)

2.5 Facsimile Number

+995 32 2915140 (this is *not* a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<cert@cert.gov.ge> This is a mail alias that relays mail to the human(s) on duty for the CERT-GOV-GE.

2.8 Public Keys and Other Encryption Information

The CERT-GOV-GE has a PGP key, whose KeyID is 44B9A839 and whose fingerprint is:

418804AAFBB8340DCA78D10C0B98BEEB44B9A839.

The key and its signatures can be found at the usual large public keyservers.

2.9 Team Members

David Kvatadze is the CERT-GOV-GE Team Leader.

Other members of the team are:

David Tskitishvili – CERT Officer

Zviad Kikvidze – CERT Officer

2.10 Other Information

General information about CERT-GOV-GE, links to various recommended security resources, can be found at:

http://www.cert.gov.ge http://www.dea.gov.ge

2.11 Points of Customer Contact

The preferred method for contacting CERT-GOV-GE is via e-mail at <cert@cert.gov.ge>; e-mail sent to this address will be handled by the responsible human. 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-GOV-GE can be reached by telephone during regular office hours. Telephone messages are checked less often than e-mail. Tel: +995 32 2915140

The CERT-GOV-GE hours of operation are generally restricted to regular business hours (10:00-19:00 Monday to Friday except holidays).

If possible, when submitting your report, use the form mentioned in section 6.

2.12 Partnership

CERT-GOV-GE is the listed team of Trusted-Introducer:

https://www.trusted-introducer.org/teams/teams-c.html#CERT-GOV-GE

3. Charter

3.1 Mission Statement

CERT-GOV-GE is a department of DEA (Data Exchange Agency) o Georgian. Agency is under supervision of Ministry of Justice of Georgia.

Our responsibly segment are Public sector and critical cyber infrastructure.

The purpose of the CERT-GOV-GE is, first, to assist government organizations in implementing proactive measures to reduce the risks of computer security incidents and to assist them in responding to such incidents when they occur.

CERT-GOV-GE also handles incidents that originate in Georgian networks and are reported by any Georgian or foreign persons or institutions.

3.2 Constituency

The CERT-GOV-GE constituency all addresses assigned to Georgian government network and critical infrastructure.

3.3 Sponsorship and/or Affiliation

CERT-GOV-GE is financially maintained by the LEPL Data Exchange Agency – DEA which it is formally a part of.

3.4 Authority

CERT-GOV-GE operates under the auspices of, and with authority delegated by, LEPL Data Exchange agency – DEA.

CERT-GOV-GE expects to work cooperatively with system administrators, network administrators, information security officers of Georgian government network and critical infrastructure. All members of CERT-GOV-GE are employees of LEPL Data Exchange Agency.

CERT-GOV-GE does its best to closely cooperate with all large Georgian ISP's abuse teams, establish direct contacts and exchange necessary data in order to prevent and recover from security incidents that affect their networks.

4. Policies

4.1 Types of Incidents and Level of Support

CERT-GOV-GE is authorized to address all types of computer security incidents which occur, or threaten to occur, in Georgian government network, Georgian critical infrastructure and in some cases other Gorgian ISP's networks.

The level of support given by CERT-GOV-GE 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-GOV-GE resources at the time, though in all cases some response will be made within two working days.

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

End users are expected to contact their systems administrator, network administrator, information security officer or department head for assistance. CERT-GOV-GE will give full support to the letter people. Only limited support can be given to end users.

CERT-GOV-GE is committed to keeping the Georgian government network informed potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-GOV-GE 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 sensible 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

In view of the types of information that CERT-GOV-GE deals with, telephones will be considered sufficiently secure to be used even unencrypted. 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, PGP 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.

Where it is necessary to establish trust, for example before relying on information given to CERT-GOV-GE, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable level of trust. Within LEPL DEA, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response

CERT-GOV-GE will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occured.
- 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 XYZ University Security and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3 Incident Resolution

CERT-GOV-GE will give advice but no physical support whatsoever to customers from outside of LEPL DEA network with respect to the incident resolution.

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

In addition, CERT-GOV-GE will collect statistics concerning incidents which occur within or involve Georgian government and critical network, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of CERT-GOV-GE incident response services, please send e-mail as per section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2 Proactive Activities

CERT-GOV-GE coordinates and mantaines the following services to the extent possible depending on its resources:

Penetration test service for public sector. Analyzing their cyber resources for vulnerabilities And reporting them.

The CERT-GOV-GE is also responsible for promouting information security awareness in different ways.

6. Incident Reporting Forms

CERT-GOV-GE had created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out, although this is never required. The current version of the form is available from: http://www.cert.gov.ge/incident_form.php

7. Disclaimers

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