CERT Bulgaria profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version **1.0** of **13 December 2010**.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3.
E-mail notifications of updates are sent to:

- All **CERT Bulgaria** members
- All **CERT Bulgaria** constituents
- The Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/)

Any questions about updates please address to the **info@govcert.bg** e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on https://govcert.bg/EN/CERTDocuments/TI-RFC2350-CERT%20Bulgaria.pdf.

2. Contact Information

2.1. Name of the Team

Full name: **Bulgarian Computer Security Incidents Response Team**
Short name: **CERT Bulgaria**
CERT Bulgaria is the CERT or CSIRT team for the **ministries, state agencies, national and regional organizations of the state administration** in **Bulgaria.**

2.2. Address

Executive Agency "Electronic Communication Networks and Information Systems"
CERT Bulgaria
6 Gurko str., Sofia 1000
Bulgaria

2.3. Time Zone

GMT+2 (GMT+3 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

+359 2 969 1680

2.5. Facsimile Number

+359 2 949 2211
Note: this is not a secure fax.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

cert@govcert.bg
This address can be used to report all security incidents to which relate to the **CERT Bulgaria's** constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication.
The current **CERT Bulgaria** team-key can be found on:
https://govcert.bg/EN/CERTDocuments/CERT%20Bulgaria%20Team.asc
and is also present on the public keyservers. The Key ID is: **0x7D3E3F6E**
Please use this key when you want/need to encrypt messages that you send to **CERT Bulgaria**. When due, **CERT Bulgaria** 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 keyservers.

2.9. Team Members

No information is provided about the **CERT Bulgaria** team members in public.

2.10. Other Information

- See the **CERT Bulgaria** webpage: **https://govcert.bg .**
- **CERT Bulgaria** is accredited by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/teams/country_AS.html .
- **CERT Bulgaria** is described in the RIPE whois database by means of an IRT-object, see http://www.db.ripe.net/whois and search for "IRT-**CERT-Bulgaria**"

2.11. Points of Customer Contact

Regular cases: use **CERT Bulgaria** e-mail address.
Regular response hours: Monday-Friday, 09:00-18:00 GMT+0200 (except public holidays in **Bulgaria**).
EMERGENCY cases: submit report through the WEB Form or send e-mail with EMERGENCY in the subject line.

3. Charter

3.1. Mission statement

The mission of **CERT Bulgaria** is to provide information and assistance to its constituencies in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur.

3.2. Constituency

The constituency for **CERT Bulgaria** is **the state administration** in **Bulgaria.**
This constituency consists of:

- **ministries**
- **state agencies**
- **national and regional organizations of the state administration**

It includes but is not limited to the following domains:

- ***.government.bg**
- ***.egov.bg**

3.3. Sponsorship and/or Affiliation

CERT Bulgaria is part of the **Executive Agency Electronic Communication Networks and Information Systems**.

3.4. Authority

The team provides information and assistance to its constituencies in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents when they occur. The team also serves as a central point of contact for other CERT teams in their attempts to escalate any incidents originating from the Bulgarian IP networks and not responded by the responsible parties. In these cases the team tries to make contact with the proper authorities in order to resolve the incidents.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. **CERT Bulgaria** itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to **CERT Bulgaria** as EMERGENCY, but it is up to **CERT Bulgaria** 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 **CERT Bulgaria**, 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.

CERT Bulgaria supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT Bulgaria 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 **CERT Bulgaria**, please make explicit what **CERT Bulgaria** can do with the information you provide. **CERT Bulgaria** will adhere to your policy, but will also point out to you if that means that **CERT Bulgaria** cannot act on the information provided.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP/GnuPG in all cases where sensitive information is involved is highly recommended.
In cases where there is doubt about the authenticity of information or its source, **CERT Bulgaria** reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

CERT Bulgaria is responsible for receiving, triaging and responding to requests and reports, and analyzing security incidents and events, involving their constituency (as defined in 3.2). **CERT Bulgaria** handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however **CERT Bulgaria** will offer support and advice on request.

5.2. Proactive Activities

CERT Bulgaria pro-actively advises their constituency in regard to recent vulnerability warnings, intrusion alerts, security advisories and trends in hacking/cracking.
CERT Bulgaria advises their constituencies on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.

6. Incident reporting Forms

Incidents could be reported by the following means of communication:

1) WEB form, available for registered users at:
https://govcert.bg/BG/IncidentHandling/Lists/RecordTable/NewForm.aspx?RootFolder=/BG/IncidentHandling/Lists/RecordTable&Source=/BG/Pages

2) By sending an e-mail with a filled in Incident reporting form available at:
https://govcert.bg/BG/CERTDocuments/Incident%20Reporting%20Form.txt

3) By sending an e-mail in plain text.

4) By phone or fax.

7. Disclaimers

None.