

RFC 2350 SRB-CERT

1 Document Information

This document describes SRB-CERT in accordance with RFC 2350.

1.1 Date of Last Update

Version 1.0, published on March 2018.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

The current version of this document is located at the following address:

<https://www.cert.rs/files/shares/RFC2350%20SRB-CERT.pdf>

It is also available upon request to info(at)cert.rs via electronic mail.

1.4 Authenticating this Document

This document has been signed with the PGP key of SRB-CERT. See section 2.8 for more details

1.5 Document Identification

Title: "RFC 2350 SRB-CERT"

Version: 1.0

Document date: March 2018

Expiration: This document is valid until superseded by a later version

2 Contact Information

2.1 Name of the Team

English name: SRB-CERT - Computer Emergency Response Team of the Republic of Serbia

Serbian name: SRB-CERT - Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima Republike Srbije (Nacionalni CERT)

2.2 Address

Regulatory Agency for Electronic Communications and Postal Services (RATEL)

Information Technologies and Cyber Security Division

Palmotićevo 2

11103 Belgrade

Serbia

2.3 Time Zone

- CET, Central European Time
(UTC+1, between last Sunday in October and last Sunday in March)
- CEST (also CET DST), Central European Summer Time
(UTC+2, between last Sunday in March and last Sunday in October)

2.4 Telephone Number

+381 11 2026 931

2.5 Facsimile Number

+381 11 3232 537 (this is not a safe fax)

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

All incidents reports should be sent to info(at)cert.rs

Use of phone and fax for reporting incidents should be avoided as much as possible.

2.8 Public Keys and Encryption Information

SRB-CERT uses PGP for digital signatures and for receiving encrypted information. The key is available on PGP/GPG keyservers and at <https://www.cert.rs/files/shares/pgp-public.txt>

Information about the key:

0x4EFE55F5DF4A1AA5

Key fingerprint = 9B8324EAAC7822AD94DF97F34EFE55F5DF4A1AA5

2.9 Team Members

Dragoslav Stanižan is the Team Manager of SRB-CERT. A full list of other members of SRB-CERT is not publicly available.

2.10 Other Information

General information about SRB-CERT in English language is available at <http://www.cert.rs/en/>.

Information in Serbian language including SRB-CERT news and bulletins is available at <http://www.cert.rs/>.

2.11 Points of Customer Contact

The preferred method of contacting SRB-CERT is via e-mail at info(at)cert.rs. Office hours for SRB-CERT are between 9:00 and 16:00 on working days. During office hours, SRB-CERT staff is available via telephone. Outside office hours team the member on duty regularly checks for reports directed to the mentioned e-mail address.

3 Charter

3.1 Mission Statement

SRB-CERT offers assistance in computer and network security incident handling and provides incident coordination functions for all incidents involving systems and networks located in Serbia. In various ways SRB-CERT helps raising awareness on issues of network and information security and provides advice and alerts to the general public.

3.2 Constituency

SRB-CERT is the Serbian national CERT and it coordinates prevention and protection from security risks in ICT systems on the national level, advises and raises cyber security awareness in the Republic of Serbia.

3.3 Sponsorship and/or Affiliation

SRB-CERT is hosted by and operates within the Regulatory Agency for Electronic Communications and Postal Service (RATEL).

3.4 Authority

The establishment of the SRB-CERT was mandated according to the Law on Information Security. SRB-CERT reports to the Ministry of Trade, Tourism and Telecommunications of the Republic of Serbia. One of its objectives is to maintain active cooperation and partnerships with all Serbian ISPs, law-enforcement bodies and other stakeholders in the field of network and information security.

4 Policies

4.1 Types of Incidents and Level of Support

SRB-CERT will gradually roll out its services, starting with announcements, alerts and incident response coordination (see 5 below).

4.2 Co-operation, Interaction and Disclosure of Information

SRB-CERT treats all information included in the correspondence as confidential. Information will only be disclosed to other parties involved in the investigation of the reported incident, in accordance with applicable Serbian

legislation. In such events any identifiable information that is not crucial to the investigation by the party involved will be anonymised.

4.3 Communication and Authentication

The preferred method of communication is via e-mail. When the content is deemed sensitive enough or requires authentication, SRB-CERT PGP key is used for signing e-mail messages. All sensitive communication to SRB-CERT should be encrypted by the team's PGP key.

5 Services

5.1 Incident Response

This service aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks. SRB-CERT will assist anyone within the constituency in handling the technical and organizational aspects of incidents.

5.2 Proactive Activities

- **Awareness-raising program “Safe on the internet” (Bezbedni na internetu)**
SRB-CERT is running the national awareness-raising program targeted at individual internet users and SMEs. Goals of the program are to provide efficient methods for risk identification and mitigation and to raise awareness via national campaigns.
- **Information services**
SRB-CERT publishes advisories for events and incidents that are considered of special importance to users in the constituency. Information is disseminated via various channels (web, mailing lists, RSS feeds, LinkedIn).
- **Training services**
SRB-CERT members shall give periodic lectures, seminars and workshops on network and information security topics.

6 Incident Reporting Forms

Reports are normally sent to the e-mail address info@cert.rs, but can also be reported via on-line form located at: <https://www.cert.rs/en/prijava.html>

7. Disclaimers

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