RFC 2350 SRB-CERT

1 Document Background

1.1 Purpose of this document

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

1.2 Date of last update

The version of this document is 3.0, published in April 2026. This version is valid until superseded by a newer version.

1.3 Distribution list for alerts

Changes to this document will not be shared through an email list or any other mechanism.

1.4 Locations where this document can be found

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

https://www.cert.rs/files/shares/RFC2350v3-SRB-CERT.pdf

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

1.5 Document authentication

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

1.6 Document identification

Title: "RFC 2350 SRB-CERT"
Version: 3.0
Document date: 24.4.2026
Expiration: This document is valid until superseded by a later version.

2 Contact Information

2.1 Team name

English name: SRB-CERT – National 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 Authority for Electronic Communications and Postal Services (RATEL)
Cyber Security, Information Technology and Finance Division
Palmotićeva 2
PAK: 106306
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 62 20 20 30

2.5 Facsimile number

Not available.

2.6 Other telecommunications options for secure voice communication

Not available.

2.7 Electronic mail address

All incident reports should be sent to info(at)cert.rs. Incidents can also be reported via online form available at https://www.cert.rs/prijava.html or via telephone number.

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 public key servers and at https://www.cert.rs/files/shares/pgp-public.txt

Key Details:
User ID: SRB-CERT
Key ID: 0x4EFE55F5DF4A1AA5
Key type: RSA
Key size: 4096 bit
Expiration: never
Fingerprint = 9B8324EAAC7822AD94DF97F34EFE55F5DF4A1AA5

2.9 Team Members

Duško Kodžić 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 https://www.cert.rs/en/. Information in Serbian language, including SRB-CERT news and bulletins, is available at https://www.cert.rs/.

2.11 Points of Customer Contact

The preferred method for contacting SRB-CERT for incident reporting is via e-mail at info(at)cert.rs. SRB-CERT office hours are from 09:00 to 16:00 on working days (Monday to Friday).

Outside office hours, the duty officer regularly monitors incoming reports sent to the aforementioned e-mail address and, in emergency cases, may also be reached by phone at:

+381 62 20 20 30.

For communication related to the submission of statistical reports by ICT operators of special importance (critical information infrastructure), SRB-CERT should be contacted via statistika(at)cert.rs, whereas questions related to the awareness raising platform “For Safer Click” should be sent to edukacija(at)cert.rs.

For general inquiries, SRB-CERT should be contacted via office(at)cert.rs.

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. SRB-CERT contributes in various ways to raising awareness on issues of network and information security, provides advice and alerts to the general public and issues early warnings for ICT operators of special importance.

3.2 Constituency

SRB-CERT is the National CERT of the Republic of Serbia and it coordinates prevention and protection against security risks to ICT systems at the national level, advises and raises cyber security awareness in the Republic of Serbia. Constituencies include ICT operators of special importance, private and public sectors, as well as citizens of the Republic of Serbia. The obligation of reporting the incidents that significantly influence information security is limited to ICT

operators of special importance. Under the Law on Information Security, ICT operators of special importance are further classified as essential (priority) ICT systems and important ICT systems.

3.3 Sponsorship and/or Affiliation

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

The National CERT of the Republic of Serbia (SRB-CERT) is a member of relevant international organizations and cooperation networks in the field of cybersecurity, such as FIRST and Trusted Introducer, thereby participating in international information-sharing on cyber threats and operating in accordance with standards applied in Europe and worldwide.

3.4 Authority

The establishment of SRB-CERT was mandated by the Law on Information Security. SRB-CERT operates under the authority of the Ministry of Information and Telecommunications of the Republic of Serbia.

One of its key objectives is to maintain active cooperation and establish effective partnerships with Internet service providers in Serbia, law enforcement authorities, and other relevant stakeholders in the field of network and information security.

4 Policies

4.1 Types of Incidents and Level of Support

SRB-CERT address all incidents involving systems and networks located in Serbia. All incidents are first prioritized according to type and severity, recommendations and advice are then provided on how the incident should be further handled. If there is a need SRB-CERT coordinates the involvement of other institutions that deal with information security in Serbia. In accordance with the Law on Information Security, incident severity is classified on a four-level scale: Low, Medium, High, and Very High.

4.2 Co-operation, Interaction and Disclosure of Information

SRB-CERT treats all information included in the correspondence as sensitive. 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 anonymized.

ICT operators of special importance are encouraged to report incidents in stages: an initial notification as soon as a significant incident is detected, progress updates as the situation develops, and a final report once the incident is resolved. SRB-CERT acknowledges receipt of reports and provides feedback, recommendations, or coordination actions at each stage as appropriate.

SRB-CERT respects and applies the Traffic Light Protocol (TLP) when handling information received from reporting parties and trusted partners. Information shared by SRB-CERT with third parties is handled in accordance with the TLP label assigned by the originating party.

4.3 Communication and Authentication

The preferred method of communication is via e-mail. When the content is deemed highly sensitive 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

The SRB-CERT provides services in the following service areas according to FIRST CSIRT Service Framework, ver. 2.1.

The National CERT, as part of the prevention of and protection against risks and incidents, maintains a register of special CERTs.

5.1 Incident Security Incident Management

Incident handling is the core service of the National CERT of the Republic of Serbia. SRB-CERT provides the following services related to incident handling:

- Information security incident report acceptance
- Information security incident analysis
- Mitigation and recovery and
- Information security incident coordination

The incident report is first examined to determine if there is an incident. Triage is done based on prioritization and categorization, after which the information in the incidents is analyzed. Recommendations on how incident could be handled are provided by SRB-CERT to its constituency. If needed, coordination between constituencies and other institutions in Serbia dealing with information security is overseen by SRB-CERT.

5.1.1 Crisis Management Support

In the event of a large-scale cyber incident affecting multiple constituencies or critical infrastructure, SRB-CERT supports national crisis management efforts by providing coordination, technical assistance, and situational awareness to relevant national authorities and stakeholders.

5.2 Vulnerability Management

SRB-CERT deals with vulnerabilities through following services:

- Vulnerability discovery / research and
- Vulnerability disclosure

The vulnerabilities are first discovered through publicly available sources (vendor announcements, security websites) or other third-party sources, as well as through incidents reports, then disseminated to general public via SRB-CERT website (https://www.cert.rs/en/preporuke.html) or shared directly with constituencies via e-mail. Vulnerabilities are assessed and prioritized using the Common Vulnerability Scoring System (CVSS).

5.3 Situational Awareness

SRB-CERT provides information about situational awareness through following services:

- Data acquisition
- Analysis and synthesis
- Communication

Information that may assist constituencies in making more informed decisions is first collected, then analyzed, and subsequently communicated through various types of reports prepared by SRB-CERT. This includes threat landscape reports that provide statistical analysis of all incidents reported to SRB-CERT, as well as reports covering incidents occurring within ICT systems of special importance.

The latter category of reports includes statistics on the incidents that had a significant impact on critical information infrastructure, as well as on those that did not have such an impact.

Near miss incidents are also reported to SRB-CERT.

SRB-CERT established MISP platform for sharing information about threats which can be used for situational awareness purposes.

SRB-CERT proactively publishes security advisories, early warnings, and public alerts through its website (https://www.cert.rs). Early warnings and alerts relevant to ICT operators of special importance are additionally distributed directly. SRB-CERT also communicates security-relevant information through social media and, where appropriate, press releases addressed to the general public.

5.4 Knowledge Transfer

SRB-CERT provides different types of knowledge transfer services:

- Awareness building
- Training and Education
- Exercises

Awareness-raising activities are conducted through publication of brochures and announcements on the SRB-CERT website, provision of interactive materials on the “For Safer Click” awareness platform, as well as through participation in and organization of information security conferences.

SRB-CERT also provides training and educational activities for various target groups, including operators of ICT systems of special importance, small and medium-sized enterprises, as well as employees of other CERTs.

SRB-CERT organizes different types of cyber exercises, such as table-top exercises, technical exercises on cyber range, and combination of table-top and technical exercises.

SRB-CERT actively supports the development of incident response capabilities across sectors of special importance through sector-oriented cyber exercises, bringing together operators to practice coordinated response to cyber incidents.

6 Incident Reporting Forms

Reports are normally sent to the e-mail address info(at)cert.rs, but can also be reported via online form available at:
https://www.cert.rs/en/prijava.html

7. Disclaimers

While all reasonable precautions are taken in the preparation of information, notifications, and alerts, SRB-CERT expressly disclaims any and all liability for errors or omissions, as well as for any direct, indirect, incidental, or consequential damages arising from the use of the information contained herein.