RFC 2350 RNIDS-CERT

1. About this document

1.1 Date of Last Update

This is version 1.01, published 2023/08/01.

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.rnids.rs/en/about-us/cert

It is also available upon request to cert(at)rnids.rs

1.4 Authenticating this Document.

English versions of this document will be signed with the RNIDS-CERT PGP key. The signature is also at:

https://www.rnids.rs/en/about-us/cert

1.5 Document identification

Title : RFC 2350 RNIDS-CERT
Version 1.01
Document date: 2023/08/01
Expiration: This document is valid until superseded by later version

2. Contact Information

2.1 Name of the Team

English name: RNIDS-CERT – Computer Emergency Response Team of Serbian National Internet Domain Registry Foundation

Serbian name: RNIDS-CERT – Centar za prevenciju i reagovanje u slučajevima zloupotrebe u .rs i .срб domenskim prostorima.

2.2 Address

RNIDS

Žorža Klemansoa 18a/I
11108 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 (0)11 7281-281)

2.5 Facsimile Number

+381 (0)11 7281-282 (this is *not* a secure fax)

2.6 Other Telecommunication

Not available.

2.7 Electronic Mail Address

cert(at)rnids.rs RNIDS-CERT team email address

2.8 Public Keys and Other Encryption Information

The RNIDS-CERT has a PGP key, whose KeyID is

B759 5435 7E1A F169

and whose fingerprint is

C067 F5F4 CA96 362A C53E 8757 B759 5435 7E1A F169

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

2.9 Team Members

RNIDS-CERT is operated by dedicated staff. It can fall back to other employes of RNIDS for special needs.

2.10 Other Information

General information about RNIDS-CERT in English language will be available cert.rnids.rs/en/.
Information in Serbian language is available at cert.rnids.rs/.

2.11 Points of Customer Contact

The preferred method of contacting RNIDS-CERT is via web form or e-mail.
Office hours of the RNIDS-CERT are from 9:00 to 17:00 on working days.
During office hours, RNIDS-CERT staff are available via telephone.
Outside office hours the team member on duty regularly checks for e-mail or web form submissions.
RNIDS-CERT follows standard office-hours on working days:
9:00 - 17:00
Outside of these hours as well as on weekends and public holidays services are offered on a best effort basis.

3. Charter

3.1 Mission Statement

The purpose of the RNIDS-CERT is, first, to assist members of Internet community:

- in implementing proactive measures to reduce abuse of the domain names in the .rs and .srb domain name space.
- to assist and respond to such incidents (domain name abuse) when they occur.
- To educate community and technical staff about DNS abuse and best practices about DNS configuration.

3.2 Constituency

The RNIDS-CERT constituency include .rs and .срб domain names.

RNIDS CERT serves Registrants and Internet users by combating abuse of the .rs and .срб (xn--90a3ac) Top Level Domain names. Also, RNIDS CERT is the central point in Serbia that raises awareness and educates Internet users about the importance of stability and security of the DNS systems.

3.3 Sponsorship and/or Affiliation

RNIDS-CERT is operated by the Serbian National Internet Domain Registry Foundation (RNIDS).

3.4 Authority

RNIDS-CERT prevents and mitigates domain name abuse incidents within its constituency and has no authority reaching further than that.

RNIDS-CERT coordinates security incidents for its constituency. It does not have any formal authority over constituency members. Rather, it operates in cooperation with judicial authorities.

4. Policies

4.1 Types of Incidents and Level of Support

RNIDS-CERT is dealing with abuse of the domain names within .rs and .srb domain space.

Response to the abuse incidents by RNIDS-CERT will be made within three working days.

4.2 Co-operation, Interaction and Disclosure of Information

RNIDS-CERT highly regards the importance of operational cooperation and information sharing between Computer Emergency Response teams and other organizations.

RNIDS-CERT will use the information provided to minimize incident impact to internet users in Serbia and will be shared to other Computer Emergency Response Teams and organizations which need to be informed. Sensitive information will only be distributed further to other teams and members by default on a need-to-know base, and preferably in an anonymized way.

RNIDS-CERT supports the Information Sharing Traffic Light Protocol; information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled accordingly.

Serbian law enforcement agencies will receive full cooperation from the RNIDS-CERT, including any information they require to pursue an investigation.
Foreign agencies should communicate through official Serbian authority’s channels.

.

4.3 Communication and Authentication

Usage of PGP/GnuPG, or other preapproved cryptographical means, 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, RNIDS-CERT reserves the right to authenticate this by any (legal) means.

5. Services

RNIDS-CERT assists and coordinates the response to cyber security incidents within its constituency to ensure incidents are handled effectively and efficiently. In case of incident, RNIDS-CERT will support with respect to the following aspects of incident management

5.1 Incident Response

RNIDS-CERT will monitor and collect information about .rs. and .srb domain names abuse, RNIDS-CERT will assist system and DNS administrators in handling the technical aspects of incidents.
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 occurred.
- Determining the extent of the incident.
- Determining the initial cause of the incident

5.1.2 Incident Coordination

- Facilitating contact with other sites which may be involved.
- Facilitating contact with SRB-CERT and/or appropriate law enforcement officials, if necessary.
- Composing announcements to users, if applicable.

5.1.3 Incident Resolution

- Coordination of removing/suspending the source of incident.
- Securing the system from the effects of the incident.
- Collection of evidence after the fact, observation of an incident in progress, etc.

5.2 Proactive Activities

RNIDS-CERT proactively advises their constituency regarding recent vulnerabilities and on matters of computer and network security.
RNIDS-CERT is not responsible for implementation, which is always left at the discretion of the constituents.

6. Incident Reporting Forms

The Form will be available at the RNIDS-CERT web site at cert.rnids.rs.

7. Disclaimers

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