RFC 2350

1. Document Information

   This document describes MUP CERT according to RFC 2350.

   1.1. Date of Last Update

   Version 1.0 - 2018/07/12

   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 CERT description document is available on the website of the Ministry of Interior of the Republic of Serbia **www.mup.gov.rs**.

2. Contact Information

   2.1. Name of the Team

   (English) Computer Emergency Response Team of the Ministry of Interior of Republic of Serbia

   (Serbian) Centar za reagovanje na napade na informacioni sistem

   Short name: MUP CERT

   2.2. Address

   Kneza Milosa 101, 11000 Belgrade, Serbia

   2.3. Time Zone

   CET

   2.4 Telephone Number

   +381 11 361 7814

   2.5 Facsimile Number

   N/A

   2.6 Electronic Mail Address

   Both incident and non-incident requests should be sent to cert@mup.gov.rs

   2.7 Other Telecommunication

   None

   2.8 Public Keys and Encryption Information

   PGP is used for functional exchanges between MUP CERT and its Partners (incident reports, alerts, etc).

   Key ID: D29C2FDB

   Fingerprint : 5700 91DA E841 5DF7 DFE7 561F 7B32 15C7 D29C 2FDB

   2.9 Team Members

Full list of MUP CERT team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other Information

N/A

2.11 Points of Customer Contact

The preferred method to contact MUP CERT team is to send an e-mail to the address cert@mup.gov.rs which is monitored by a duty officer 24/7.

Urgent cases can be reported 24-7 by phone on +381 11 361 7814

Hours/Days of Operation: 07.30 to 15.30 Monday to Friday (except holidays).

Out of office hours operation in case of emergency.

3. Charter

3.1 Mission Statement

MUP CERT mission is to support and protect ICT systems of Ministry of Serbia in order to keep private and sensitive data stored in its databases safe and reliable. The scope of MUP CERT's activities covers prevention, detection, response and recovery in cases of intentional and malicious attacks as well as in cases of unintentional misconducts that could endanger the integrity of its ICT assets and harm the interests of the citizens of Serbia.

MUP CERT is ready to serve as the CERT of last resort in Serbia.

3.4 Constituency

The constituency of MUP CERT are employees and ICT systems of Ministry of Interior of Republic of Serbia.

3.5 Sponsorship and/or Affiliation

MUP CERT is part of Ministry of Interior of Republic of Serbia.

3.6 Authority

The establishment of MUP CERT is mandated by Law on Information Security and Rulebook of Organization of the Ministry of Interior.

4. Policies

4.1 Types of Incidents and Level of Support

The MUP CERT is authorized to address and fully resolve all types of computer security incidents that affect Ministry of Interior systems and data.

4.2 Co-operation, Interaction and Disclosure of Information

MUP CERT highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, and also with other organizations which may contribute to the better cyber security.

MUP CERT treats all information included in the correspondence as confidential. Information will only be disclosed to other parties involved in the investigation and /or resolution of the reported incident.

MUP CERT operates within the confines imposed by Serbian legislation.

4.3 Communication and Authentication

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back or mail-back .

5. Services

5.1 Incident Response

MUP CERT assists local network and security administrators in handling the technical and operational aspects of incidents.

5.1.1. INCIDENT TRIAGE

Determining the scope of the incident, its priority, and possible impact;

Determining the starting resources necessary to tackle the problem.

5.1.2. INCIDENT COORDINATION

Engage all internal resources necessary to investigate the incident and to take the appropriate steps ;

Contact external parties which can help resolve the incident;

Contact other parties that might be endangered by incident.

5.1.3. INCIDENT RESOLUTION

Provide advice to network and system administrators on appropriate actions;

Provide assistance in evidence collection and data interpretation;

If necessary, MUP CERT is deployed on site to resolve the problem.

5.2 Proactive activities

MUP CERT provides announcements, warnings and alerts to the constituency of MUP CERT, both system administrators and employees, and to the other CSIRT teams in the country.

MUP CERT is involved in raising security awareness of its constituency.

6. Incident Reporting Forms

Please provide MUP CERT at least with the following information:

- contact details and organizational information – name of person and organization name and address, email address, telephone number;
- IP address and observation.

7. Disclaimers

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