RFC 2350 - CSIRT.MIL.SK PROFILE

1 Document Information

This document contains a description of CSIRT.MIL.SK according to standard RFC 2350. It provides basic information about the CSIRT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 1.0, published on December 15th, 2017.

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 CSIRT.MIL.SK members
- The Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/)

Any questions about updates please address to the CSIRT.MIL.SK e-mail address.

1.3 Locations where this document may be found

The current version of this CSIRT/CERT description document is available on the CSIRT.MIL.SK site; URL: http://vs.mosr.sk/o-nas/documents/RFC 2350.docx .
Please make sure you are using the latest version of this document.

2 Contact Information

2.1 Name of the Team

CSIRT.MIL.SK - Military Computer Security Incident Response Team Slovakia

2.2 Address

Military Intelligence
Ministry of Defence of the Slovak Republic
Kutuzovova 8
832 47 Bratislava
Slovak Republic

2.3 Time Zone

We are located in the central European timezone (CET) which is GMT+0100 (+0200 during day-light saving time).

2.4 Telephone Number

+421 960 319 599

2.5 Facsimile Number

+421 960 314 688

2.6 Other Telecommunication

Not available at the moment.

2.7 Electronic Mail Address

Official e-mail address: cyber@mosr.sk
Address for security incident reporting: cyber@mosr.sk

2.8 Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication.
CSIRT.MIL.SK PGP Key:
User ID: Ministry of Defense of the SR (MoD SVK) <cyber@mosr.sk>
Key ID: 0xEAF97FCA
Key Fingerprint: FE0E E37F BF17 16D8 A110 04BB 1D55 8CA9 EAF9 7FCA

The current CSIRT.MIL.SK team-key can be found on http://vs.mosr.sk/o-nas/documents/cyber.asc and is also present on the public key-server https://keyserver.pgp.com/(Ministry of Defense of the SR, cyber@mosr.sk).

2.9 Team Members

No information is provided.

2.10 Other Information

CSIRT.MIL.SK is registered as an "ACCREDITATION CANDIDATE" by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/directory/teams/csirtmilsk.html

2.11 Points of Customer Contact

The preferred method for contacting CSIRT.MIL.SK is via e-mail.
For incident reports and related issues please use cyber@mosr.sk.

CSIRT.MIL.SK operation hours are generally restricted to local regular business hours: Mon-Fri, 7 a.m. – 3:30 p.m. CET/CEST.

3 Charter

3.1 Mission Statement

The purpose of CSIRT.MIL.SK is to coordinate cyber security efforts and incident response to IT-security incidents on the military level in the Slovak Republic and to provide cyber defence support to a strategic defence infrastructure and a national critical infrastructure.

3.2 Constituency

Constituency of the CSIRT.MIL.SK involves Ministry of Defence of the Slovak Republic, its subordinate organizations and a part of the national critical infrastructure that is considered to be a strategic defence infrastructure.

3.3 Sponsorship and/or Affiliation

CSIRT.MIL.SK is a Military CSIRT (Computer Security Incident and Response Team) of Ministry of Defence of the Slovak Republic established in September 18th, 2013 as special department of the Slovak Armed Forces. Based on the Ministerial Decision it has been integrated under the Military Intelligence (a special service under the Ministry of Defence of the Slovak Republic) in November 1st, 2016 and renamed from CSIRT.MIL to CSIRT.MIL.SK.

3.4 Authority

The team provides response to cyber security incidents on behalf of their constituency and has no authority reaching further than that.

4 Policies

4.1 Types of Incidents and Level of Support

The CSIRT.MIL.SK is authorized to address all types of computer security incidents which occur in its constituency. No direct support is given to end-users, as they are expected to contact their system administrators based on the internal organization policies.

CSIRT.MIL.SK is committed to keep the constituency informed of potential vulnerabilities and existing threats, and where possible, will inform them of such threats and vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

According to our internal organization policies and procedures, ALL incoming information is handled by CSIRT.MIL.SK based on the level of classification (public, sensitive, classified) and ALL incoming classified information is processed in separated environment based on the level of its classification (restricted, confidential, secret, top secret).

CSIRT.MIL.SK supports also the Information Sharing Traffic Light Protocol (TLP). Information labeled with TPL tag will be handled appropriately.

By default, the information provided by the CSIRT community will be used by CSIRT.MIL.SK to respond to current threat. Information will be distributed further only to the appropriate parties based on the classification and on a need-to-know base in an anonymous fashion (if not stated by the sender otherwise).

4.3 Communication and Authentication

1. For public communication not containing sensitive/classified information, CSIRT.MIL.SK might use conventional methods like unencrypted phone, e-mail or fax.
2. For sensitive communication, PGP-encrypted e-mail or telephone might 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) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.
3. There is a possibility to communicate via classified communication channels using NSWAN/CRONOS.

5 Services

5.1 Reactive Services

CSIRT.MIL.SK is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). It will provide assistance or advice with respect to the following aspects of incident management:

- Alerts & Warnings
- Incident response and incident response support
- Vulnerability handling
- Artifact handling

5.2 Proactive Activities

CSIRT.MIL.SK pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.

- Announcements about existing vulnerabilities
- Security network monitoring
- Threat intelligence sharing
- Threats Monitoring in the field of ICT

5.3 Security Quality Management services

- Education and awareness rising

6 Incident Reporting Forms

There are no forms available.

7 Disclaimers

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