



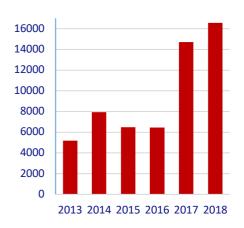
VULNERABILITY REPORTING GUIDELINE



#INTRODUCTION

The National Institute of Standards and Technology (NIST) operates the National Vulnerability Database (NVD). Within the year 2018 altogether 16 555 vulnerabilities marked with CVE code were recorded among all existing software products and platforms. It means that on average at least 45 vulnerabilities of different severity were discovered every day. Disclosure and removal of vulnerabilities should be subject to certain rules in order to eliminate the abuse of a particular vulnerability which may affect not only in the functionality of a vulnerable system or service but can particularly have direct impact on users in the form of data loss, alteration or leakage, denial of service or other serious facts.

Vulnerabilities in NVD Database



Four reasons why vulnerabilities exist:

#1

Security is often contrary to pressure on new application and service functions and the speed of development and deployment. The benefits of a safe design and the associated savings are not seen until later, in operation. However, this connection is often underestimated by application creators.

#2

Software development combines the knowledge of programming language, libraries, databases, communication protocols (against other applications, databases, servers, users) and file formats. It is extremely difficult for a programmer to acquire and maintain cuttingedge knowledge of the latest security practices in all of these areas. It is practically impossible to think of all cases and make no mistake, even if the programmer knows them.

#3

Even if the programmer adheres to all conceivable security recommendations in his own code and does not make any mistakes, a brand new vulnerability category is sometimes revealed or the external environment changes, which result in a redesign of the application in order to adapt to a new situation.

#4

Unfamiliar mistakes from used external libraries and operating system are also introduced into the applications. These may cause the occurrence of exploitable vulnerabilities even if the author complied with all security policies.

The National Cyber Security Centre SK-CERT publishes this Guideline as a recommended procedure for vulnerability reporting and can be used by security researchers, cyber activists as well as ordinary citizens. This guideline is also suitable for vulnerability reporting in products and services of the National Security Authority and the National Cyber Security Centre SK-CERT.





#VULNERABILITY

Generally, the vulnerability is any circumstance that reduces the resistance to threats.

The vulnerability is an intentional or unintentional error of a software product, hardware, or process that allows unauthorized people or processes to access assets (data, software, hardware, people, etc.), prevents authorized access to assets, or allows unauthorized people and processes to avoid detection.

Abuse of the vulnerability also means:

- # the ability to execute a random code (unauthorized, unplanned, malicious, etc.)
- # to acquire administrative privileges or privileges of the other user group or a user
- # a denial of service or a product
- # to gain unauthorized access to read or modify sensitive data

#CVE Code

If the vulnerability of a product or service is disclosed, the CVE code (Common Vulnerabilities and Exposures Code) is assigned to the vulnerability after the reporting process to a responsible entity (most commonly a manufacturer or an operator). This code can be assigned by one of the participating CSIRT teams, Bug Bounty programmes, manufacturers, security researchers or the MITRE organization as a primary CVE numbering authority. The CVE code is used for central record keeping of all known vulnerabilities.



#CVSS

CVSS System (Common Vulnerability Scoring System) is a metrics that allows to compare the severity of different vulnerabilities. The CVSS score is a number from 0 to 10, calculated according to exact formulas, including abuse patterns, effects on confidentiality, integrity and availability, and other criteria.

CVSS metrics can be used not only to determine the vulnerability severity but also to prioritise its handling or removal. The current version of CVSS metrics (v 3.1) recognizes four categories of vulnerabilities:

Score	Severity
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

CVSS can be calculated with the calculator which can be found on the link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Methodology of CVSS version 3.1 can be found on the link:

https://www.first.org/cvss/specification-document



#WHY

#Why to report vulnerabilities?

The security of each system is defined by its weakest link. Vulnerabilities open the door for attackers to get inside the system, to sensitive data, personal data, and in many cases to the overall control of the infected system.

If the vulnerability information was not reported to the author of the software, hardware manufacturer or service provider, these services would be exposed to the risk of attacks from the parties who know the vulnerability. Conversely, if the vulnerability information was publicly published before the manufacturer was given the chance to fix the vulnerability and distribute security updates, patches or fixes to users, this could lead to panic and mass abuse of the vulnerability by attackers.

Responsible and coordinated vulnerability reporting is the best way to eliminate the vulnerability with minimal adverse effects. At the same time, it enables the reporter to get credit from the experts and possible bug bounty. CSIRTs may provide anonymity to the reporter, if there is a need, or to ensure all necessary steps in the process. Reporting the vulnerabilities in a timely manner enables the manufacturer to minimize the impact on users and to prevent property and reputation damage.

Benefits for the reporter:

- # By reporting the vulnerability, pursuant to rules, the vulnerability abuse by a dangerous attacker can be prevented
- # The affected entity as well as users of vulnerable system or service can be helped
- # The reporter practises his skills in cybersecurity

Benefits for the affected entity:

- # The affected entity learns about the issue to which it can immediately respond and prevent harmful effects
- # By following the reporting rules it improves its products and services offered to customers
- # The affected entity builds a reputation in cyber community



#RULES

Recommended procedure for the reporter

- # Report the vulnerability to the National Cyber Security Centre SK-CERT as soon as it is detected in order to minimize the risk of abuse by the attackers.
- # For confidentiality, it is recommended to encrypt the communication via PGP.
- # The vulnerability report must include a detailed description of the problem. Suggestion of the vulnerability solution is also possible.
- # It is recommended to include a detailed contact information in the report, along with the means of secure communication (e. g. PGP fingerprint).
- # SK-CERT may assist the reporter by taking further steps:
 - * to assess a reported vulnerability from an expert viewpoint,
 - * to register CVE number for vulnerability,
 - * to identify entities concerned and their respective contacts (a manufacturer, national CSIRTs, affected users),
 - * to contact entities concerned either with the reporter identity or with the reporter anonymity.
- # The reporter may specify a vulnerability removal period for the affected entity during which the vulnerability is not disclosed publicly. If the entity does not respond to the report and the deadline expires, the reporter may disclose the vulnerability publicly. It is a good practice to add vulnerability solution methods or mitigation to the vulnerability report. The default period is 30 to 90 days, depending on the nature of the vulnerability.
- # The reporter should avoid the following activities in the vulnerable system:
 - * install a malicious code
 - * copy, alter or delete the data
 - * make changes in the system
 - * sign in the system repeatedly or share the ability to sign in with the third parties
 - * use other methods (e. g. brute force) for deeper penetration into the system
- # These activities are illegal and may be considered a crime or an offense.





#RULES

Recommendations for affected entities (manufacturer, owner, provider of vulnerable system or service)

- # A company should have implemented:
 - * a process of vulnerability reporting (within the process each reported issue should be assessed and not just limited to the vulnerabilities with higher severity),
 - * a process of vulnerability prioritisation and management,
 - * a process of vulnerability disclosure to the public.
- # The response to each report should be prompt and adequate to the reported vulnerability.
- # The vulnerability management process should be given a high priority and vulnerabilities should be fixed in the next update.
- # The vulnerability management process should also include identifying potential victims and the method of their notification.
- # If the vulnerability is to be disclosed to the public, the company will determine the date of disclosure and notify the reporter if the vulnerability was not detected by the company. After consulting the reporter, it will also choose an appropriate channel for vulnerability disclosure to the community and the public.
- # The company may reward the reporter for reporting the vulnerability. It may also "offer a reward" for finding vulnerabilities in its products. This procedure is recommended to increase the security of the company's products and services.
- # Vulnerability reporting should be seen as an opportunity to improve products and a chance to learn about the vulnerability earlier than its abuse causes damage to the user, operator or manufacturer of the product or service. Therefore, it is recommended to treat the reporter gratefully as a person who wants to help as a friendly co-worker. This, of course, does not preclude legal action if the reporter's actions are manifestly unethical or illegal.





#AUTHORITY

What is expected from Cyber Security Authority/Authorities?

- # National Cyber Security Authorities, in Slovakia it is the National Cyber Security Centre SK-CERT, should issue standards and recommendations regarding vulnerability reporting, management and vulnerability disclosure to the public.
- # In case of vulnerability reporting to the Cyber Authority, coordinate the procedure with the affected entity and the reporter.
- # If necessary and in accordance with applicable legislation, ensure the anonymity of the reporter in order to be protected against unauthorized recourse or intimidation from the side of the manufacturer or operator of the vulnerable product or service.
- # Promote vulnerability reporting by raising security awareness and motivating companies, security researchers and other entities.
- # When reporting the vulnerability that is directly related to the Cyber Authority, proceed in accordance with the recommendations for the affected entity.

#Contact details of the National Cyber Security Centre SK-CERT



National Security Authority

Budatínska 30 | 851 06 Bratislava | Slovenská republika

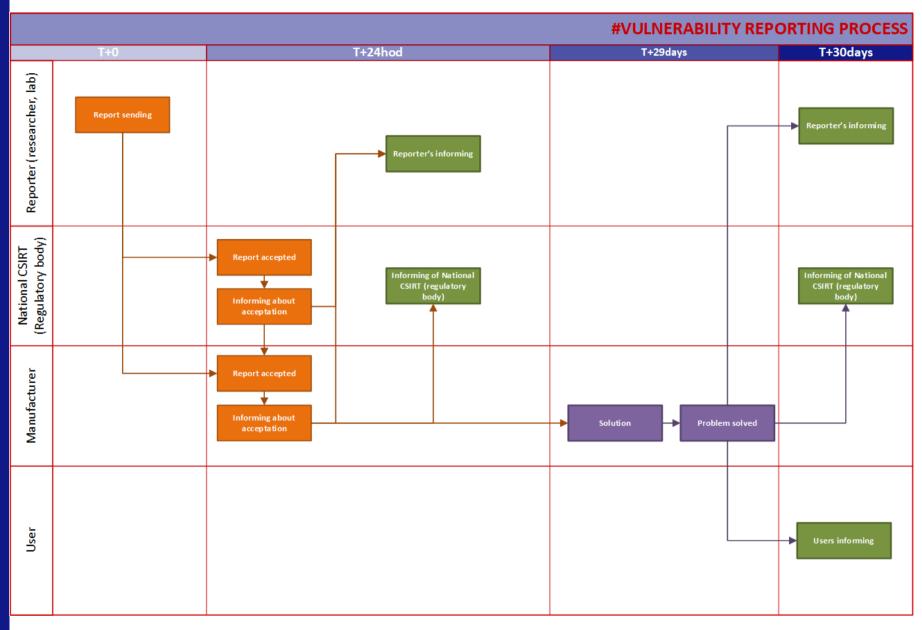
tel.: +421 2 6869 2915 | mob.: +421 903 993 706

e-mail: incident@nbu.gov.sk

PGP Fingerprint: D66E 619A E83A 8802 51A6 5AC7 CF74 96BD 1A1A 0ACD

web: https://www.sk-cert.sk | https://www.nbu.gov.sk







#ABOUT THE DOCUMENT

This document was created and is maintained by the National Cyber Security Centre SK-CERT of the National Security Authority.

About us

With designation of the National Security Authority (hereinafter referred to as "the Authority") as the central government body for cyber security, the Authority has established the Slovak Computer Emergency Response Team (SK-CERT), which was transformed to the **National Cyber Security Centre SK-CERT** unit. The unit provides national and strategic activities in the field of cyber security management, threat analysis as well as coordination of security incident handling at national level.

The Act No. 69/2018 Coll. on Cyber Security and on amendment and supplementing of certain acts came into force on 1 April 2018. It defines the roles, rights and obligations in the field of cyber security. At the same time, this law determines the role of the Authority as the National CSIRT Unit, and that is being executed by the independent unit, the National Cyber Security Centre SK-CERT.

This document was created with the support of the National Cyber Security Centre of the Netherlands which issued several documents regarding the coordinated vulnerabilities reporting.

More about this document are available on:

https://www.sk-cert.sk/en/vulnerability-reporting/index.html

#REVISIONS

VERSION	DATE	NOTE
1.0	15.9.2019	First version of the document

