Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSC

NCSC – VULNERABILITY MANAGEMENT

Vulnerability disclosure management

A guide for companies and organisations

01.02.2024

Contents

1 Introduction ... 3
1.1. Vulnerability disclosure objectives ... 3
2 Elements of the NCSC guide ... 4
2.1 Communication ... 4
2.1.1 Making specific contact details available ... 4
2.1.2 Technical requirements ... 4
2.1.3 Process ... 5
2.2 Guidelines ... 6
2.3 Security.txt ... 6
2.3.1 Example "security.txt" on the NCSC website ... 7
3 Links ... 8

1 Introduction

If an IT vulnerability is discovered in your company's or organisation's systems or products by an internal or external party, it should be possible for them to report this immediately to the relevant IT unit in your company/organisation by following a clearly defined process.

With a clear and easy-to-understand reporting procedure, companies and organisations of all sizes can obtain information on vulnerabilities directly, meaning that they can remedy them more quickly and in a more targeted manner. A clearly defined reporting procedure shows that the company/organisation takes security issues seriously and strives to continuously improve its systems and products.

This NCSC vulnerability disclosure guide is aimed at companies and organisations and is intended to help them implement such a reporting procedure in their operations. It comprises the three essential components: communication, guidelines and "security.txt".

This guide is largely based on the international standard for vulnerability disclosure (ISO/IEC 29147:2018). It defines the techniques and guidelines that can be used for receiving vulnerability reports and disclosing information on how to remedy vulnerabilities. ISO/IEC 29147:2018 was adopted by the European Committee for Standardization (CEN) on 3 May 2020.

1.1. Vulnerability disclosure objectives

Vulnerability disclosure enables, on the one hand, vulnerabilities to be remedied and, on the other hand, more conscious risk decisions to be made. According to ISO/IEC 29147:2018, the priority objectives of vulnerability disclosure include:

- Reduce risk by remedying vulnerabilities and informing users.
- Minimise damage and costs.
- Provide sufficient information to users to assess the risks posed by the vulnerabilities.
- Define the expectations of all stakeholders to facilitate interaction and coordination between them.

2 Elements of the NCSC guide

This guide contains three essential elements of the vulnerability disclosure process:

2.1 Communication

2.1.1 Making specific contact details available

It is crucial that communication is quick and straightforward for all stakeholders.
If employees of your company or organisation, security researchers, ethical hackers, the NCSC or the general public are aware of a technical vulnerability in your company or organisation, it is crucial that they are able to quickly find and contact the responsible IT unit to remedy the vulnerability.

Often this specific (contact) data is not available. In many cases, only a central telephone number or a general email address is listed on the relevant website. As a result, the reporting party has to ask around to find the right contact person and explain the problem multiple times, often wasting valuable time. By the time the information reaches the person in charge, it may already be too late. It is also often the case that the information is ignored and not forwarded, and the responsible office is not informed about the vulnerability. This is frustrating for the reporting party, but also problematic for the affected company/organisation and a wasted opportunity to improve its own cybersecurity.

To counteract this problem, the contact details of the person responsible for IT must be easy to find or, at least, a reporting process should be defined within the company. The NCSC recommends including their contact details on the "contact" page of the website. In addition, the contact options should be recorded in a specially created file "security.txt" and stored on the website (see section on "security.txt").

2.1.2 Technical requirements

A specially created email address or web form ensures that the reporting party's information is forwarded to the right place in your company/organisation.

If a web-based reporting procedure (e.g. web form) is used, data transmission must be encrypted, e.g. using TLS (HTTPS). Communication via email should use encrypted and signed methods such as S/MIME or PGP. The public keys required for this should be stored on the website and be accessible.

An example of a web form can be found on the NCSC website:

https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html

2.1.3 Process

This guide defines four steps in the vulnerability handling process:

Report received:
If you receive a report of a possible vulnerability, you should acknowledge receipt as soon as possible, but at the latest within seven calendar days, and thank the person who made the report. The response may be automatically generated, but should be sincere. It should include a tracking number or identifier and preliminary status information.

Verification:
This is followed by an assessment and verification of the reported vulnerability. In the case of a high number of reports, triaging should occur based on the risk assessment of the vulnerabilities. After the assessment has been completed, we recommend that you inform the reporting party of the outcome of this initial evaluation.

Vulnerability management:
During the subsequent stages of the vulnerability assessment, you should communicate with the reporting parties on a regular basis. This communication should include the following information:

- Status updates
- Relevant new information
- Changes to existing plans
- Timetable for disclosure

Publication:
Communication is the essential element. An easy-to-find contact channel as well as prompt, transparent and appreciative communication throughout the vulnerability management process will encourage commitment and motivation among the reporting parties.

2.2 Guidelines

By setting clear guidelines, you define what you expect from someone who reports a vulnerability and what the reporting party can expect from your company/organisation in return. This means that the reporting parties can work with you within an agreed framework.

ISO/IEC 29147:2018 sets out mandatory and recommended disclosures for vulnerability disclosure guidelines:

- Contact mechanism, e.g. link/email or web form **(mandatory)**
- Information to be provided in the vulnerability report, see also ISO/IEC 29147:2018, Annex B **(recommended)**
- Communication requirements **(recommended)**
- Recognition **(recommended)**
- Legal aspects **(recommended)**

An example of such guidelines can be found on the NCSC website:
https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html

Further examples of such guidelines can be found in ISO/IEC 29147:2018, Annex A.

2.3 Security.txt

The "security.txt" standard enables the correct security contact in a company/organisation to be found quickly. The standard requires a text file entitled "security.txt" to be saved in the predefined "/.well-known" directory on the web server of the website. As a minimum, this file contains the contact details that can be used to get in touch with the person responsible for the security of a website, or of a company or organisation. In addition, links to encryption keys, security guidelines, special vulnerability disclosures and bug bounty programmes can also be stored.

Since April 2022, this standard has also been officially anchored as "RFC 9116" and is increasingly used globally on the internet by both tech companies and government organisations.

The "security.txt" file contains mandatory and optional information:

What	Description	Mandatory	Optional
Contact	A link or email address where the organisation or company can be contacted regarding security issues. Remember to include "https://" and "mailto:" for URLs.	X	
Expiry date	Date and time when the contents of the security.txt file should be considered out of date. Make sure you update this value regularly and check your file on an ongoing	X	

	basis.		
Preferred language	A list of languages, separated by commas, spoken by your IT office. You can specify more than one language		X
Encryption options	A link to a key (e.g. PGP or S/MIME) that security researchers can use to communicate securely with you.		X
Acknowledgements	A link to a web page where the company/organisation expresses its gratitude to security researchers who have reported a security issue to you and would like to be mentioned in this way. Remember to include "https://".		X
Link to the security.txt file	The URLs for accessing your security.txt file. It is important to include these when you digitally sign the security.txt file so that the location of the security.txt file can also be digitally signed.		X
Policy	A link to a guideline that describes how security researchers should proceed when reporting security issues to you. Remember to include "https://".		X
Job offers	A link to all security-related job offers in your company. Remember to include "https://".		X

This list is not exhaustive. For more information, see the RFC9116 standard (see Appendix).

2.3.1 Example "security.txt" on the NCSC website

https://www.ncsc.admin.ch/.well-known/security.txt

```
# In the event that you have discovered a technical vulnerability in an IT system of the federal government,
# we encourage you to report it to the National Cyber Security Centre NCSC using the Coordinated Vulnerability Disclosure program.
# We forward your request to the appropriate unit.
# If you are interested in participating in the NCSC bug bounty programs you can apply here: https://www.bugbounty.ch/ncsc

Contact: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html
Contact: mailto:incidents@ncsc.ch
Expires: 2024-12-31T23:59:59.000Z
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/pgp_ncsc_incidents.asc.download.asc/NCSC_Incidents.asc
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/smime_incidents_ncsc_ch_22.cer.download.cer/smime_incidents_ncsc_ch_22.cer
Preferred-Languages: en, de, fr, it
Canonical: https://www.ncsc.admin.ch/.well-known/security.txt
Policy: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html
```

3 Links

ISO/IEC 29147:2018 Standard: Vulnerability disclosure
https://www.iso.org/standard/72311.html

ENISA - Coordinated Vulnerability Disclosure policies in the EU
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

IETF - RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure
https://www.ietf.org/rfc/rfc9116.pdf

OSCE learning: cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure
https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

NCSC hot topic: Purported security researchers press for rewards
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/wochenrueckblick_38.html