CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

COORDINATED VULNERABILITY DISCLOSURE POLICIES "CVDP"

Coordinated vulnerability disclosure policies "CVDP"

Any network or information system may contain vulnerabilities. These may be discovered by people with good or malicious intentions. However, the fear of being prosecuted often prevents people with good intentions ("ethical hackers") from reporting vulnerabilities which they discover.

Gaining or attempting to gain unauthorized access to an IT system is punishable even if the IT system is insecure and the person is acting with good intentions. However, if the person is authorized to access the IT system, the legal rules are different.

When an organisation applies a coordinated vulnerability disclosure policy (hereafter "CVDP") and/or a bug bounty program, that organisation may grant at least partial access to the computer systems concerned.

Indeed, the organisation can either engage a company to audit the security of their information systems (via a security audit for example) or call on "ethical hackers" (via a CVDP or a bug bounty).

A coordinated vulnerability disclosure policy*[1] *("CVDP") *is a set of rules pre-determined by an organisation responsible for IT systems that allows participants[2] (or "ethical hackers"), with good intentions to identify possible vulnerabilities in its IT systems , or to provide the organisation with all relevant information about them. These rules, usually published on a website, make it possible to define a legal framework for the cooperation between the responsible organisation and participants under the policy. These rules should ensure, inter alia, the confidentiality of the information exchanged and provide a responsible and coordinated framework for any disclosure of discovered vulnerabilities.*

[1] *Also called "responsible disclosure policy": we prefer the term "coordinated" rather than "responsible" as it avoids any confusion with the concepts of civil liability and emphasizes the reciprocal nature of the process.*

[2] *These could be, for example, cyber security researchers or users. Participants may be subject to selection by a third party who acts as a confidential adviser ("coordinator").*

***A Vulnerability Rewards Program (or "bug bounty program")**[3] relates to all rules set by a responsible organisation to give rewards to participants who identify vulnerabilities in the technologies it uses. This reward can be a sum of money, but also a gift or simply public recognition (public ranking among the best participants, publication, conference, etc.). This is a coordinated vulnerability disclosure policy that provides for a reward to be paid to the participant according to the amount, importance or quality of the information transmitted. This policy is more attractive to potential participants and often leads to better results for the organisation. The organisation may, for example, use a bug bounty platform that provides technical and administrative assistance to manage of its vulnerability detection reward programme (coordinator role)[4].*

Currently, many organisations have already CVDP implemented with or without a bug bounty programme.

In order to help organisations that wish to implement a CVDP, the Centre for Cybersecurity Belgium (CCB) has developed this brochure, a Guide (in two parts) and an example of policy.
These documents are available on the CCB website.

Moreover, the CCB itself has adopted and published its CVDP on its website (www.ccb.belgium.be/en/vulnerability-policy).

[3] *"Programme de récompense pour la découverte de vulnérabilités" in French or « beloningsprogramma voor het opsporen van kwetsbaarheden » in Dutch.*

[4] *See for example: www.intigriti.com (Belgium); www.yeswehack.com, www.yogosha.com (France); www.zerocopter.com (NL); www.hackerone.com, www.bugcrowd.com (USA), etc.*

This folder provides an overview of the concepts, objectives, legal issues and good practices surrounding the adoption of coordinated vulnerability disclosure policies ("CVDP") in the current state of Belgian legislation - see for more details the Guide CVDP (part I and II) and the example of policy.

We would like to point out that the documents drawn up by the CCB in no way change the existing legal rules. Unauthorized intrusion into a third party's computer system, even with good intentions, is a criminal offence.

Participants in a CVDP must be aware that they cannot invoke a general exclusion of liability when participating in that policy: they must act prudently and scrupulously comply with all the conditions of the policy as well as the applicable legal provisions.

For organisations:

What are the advantages for your organisation of adopting a CVDP ?

a) provide a legal framework for useful, fair, effective, legal and budget-friendly cooperation.

The coordinated vulnerability disclosure policy is a type of accession agreement outlining all contractual provisions for the responsible organisation and subsequently accepted by the participant when it freely decides to participate in the existing program. The adoption of such a policy clarifies the participants' legal position. After all, they can demonstrate that they have prior authorization to access the IT systems concerned and therefore do not intrude into those systems unlawfully, provided that the conditions set out in the policy are met (see Coordinated Vulnerability Disclosure Policies Guide. Part II: Legal aspects).

The coordinated vulnerability disclosure policy provides an opportunity for continuous and effective monitoring of the security of systems or equipment. Obviously, the policy is more attractive and effective when the responsible organisation decides to give rewards to participants, depending on the importance and quality of the information provided (as part of a Vulnerability Rewards Program or bug bounty program). Even when the organisation grants rewards and calls on an external coordinator (ethical hacking platform), setting up costs of a coordinated vulnerability disclosure policy are more budget-friendly than the performing audits by external companies.

b) Improving the security of IT systems and driving research

In addition to other technical and organisational measures, setting up such a cooperation may be an appropriate measure to prevent incidents that would compromise the security of its network and information systems. It has the undeniable advantage of identifying and resolving vulnerabilities before a security incident occurs. In addition to increasing security, this type of policy can also improve knowledge about cyber security and drive research in this field.

c) Ensuring users have confidence in IT technologies

Implementing a CVDP demonstrates to the public and users that the responsible organisation attaches great importance to the security of its IT technologies. After all, this approach implies a commitment by the organisation to process the information provided by the participants and to try to remedy the vulnerabilities identified, or at least to inform the users of the risks. This commitment can also be a marketing tool and the organisation can refer to this in its communication. Trust in IT systems is certainly an important bonus for users or consumers.

d) Guaranteeing confidentiality

Full disclosure of a vulnerability, while it still exists among many users, poses a major IT security risk. Indeed, third parties with bad intentions can develop and disseminate specific tools to exploit this vulnerability. Disclosing security problems may also harm the reputation of the responsible organisation and undermine user confidence in the technologies concerned. The interest of a CVDP therefore lies in the establishment of a legal framework that reinforces confidentiality and provides the best possible framework for a possible public disclosure.

e) Ensuring better compliance with legal obligations in the area of IT security

By implementing a coordinated disclosure policy, the organisation demonstrates its commitment to comply with its legal obligations to ensure the security of its network and IT systems: General Data Protection Regulation EU No 2016/679 ("GDPR"), Act of 7 April 2019 establishing a framework for the security of network and IT systems of general interest for public security ("NIS Act"), Civil Liability Regulation, Economic Law Code, etc. (See Guide Part I: Good practices).

Every organisation can choose the scope of the mutual obligations in its CVDP. Nevertheless, we recommend that you include at least the following conditions:
Each organisation can set the precise rules, provided that certain elements are included, so that the policy can be can fully achieve its legal effects.
Thus, we recommend to take the following measures:

- **Authorised persons:** have the policy approved by a person authorized to legally represent your organisation (e.g. the director).
- **Publicity:** the content of your CVDP should be available and accessible by the participant: either on your website or on the website of a coordinator (e.g. a bug bounty platform). If possible, it should be written in the different languages of your website. We recommend a concise and clear but complete text.
- **Contact point:** clearly identify a contact point or use an online form. Then communicate as often and as effectively as possible with the participants. They may be able to help you find out if your technical solution is working.
- **Coordinator:** it can be very efficient to appoint a coordinator. For example, the use of using a bug bounty platform may allow you to receive a larger number of vulnerabilities. If the participants in the policy or the designated coordinator do not respond, you can call on the CCB (vulnerabilityreport@cert.be) as coordinator by default.
- **Security and confidentiality of communications:** ensure the security and confidentiality of your communications.
- **Scope:** clearly state to which sites, products, devices, services, systems and networks applies your CVDP? Choose the scope of your policy carefully, based on the elements of your system that you are technically able to monitor. Exclude all systems that

depend on third parties who have not explicitly agreed to the rules of your CVDP. If you are unable to verify that the CVDP has been respected for some components of your system, avoid including them in the scope of your CVDP. What is not explicitly mentioned in the scope does not, in principle, fall within the scope of the policy.

- **Conditions:** clearly state what the participant can and cannot do in order to prove the existence of a suspected vulnerability. Any changes to data in the computer system should be minimal (e.g. the presence of system should be minimal (e.g. the presence of "visit logs"). Explicitly prohibit the installation of malware or viruses, passwords stealing, deleting or changing system settings, use of denial of service ("DDOS") attacks, social engineering attacks, phishing, spamming, etc. Exclude the use, possession, revelation or disclosure of the content of non-publicly available communications or data from a computer system, which the participant could not reasonably be unaware that it was obtained illegally (such as stolen passwords published on the internet).
- **Notification:** clearly specify the desired information from the participant (type of vulnerability, details of the configuration, operations performed, tools used, date of testing, evidence, IP address or URL of the affected system, screenshot, contact details, etc.). Set response times in advance for information about a vulnerability and the other phases of the of the procedure. Communicate these deadlines also during each contact. Retain the right to flexibility according to the complexity, urgency and extent of the vulnerability.
- **Proportionality:** Require participants not to exceed reasonable limits to prove a vulnerability. This also implies that the availability of the responsible organisation's services cannot be disrupted by the researches.
- **Confidentiality:** enforce confidentiality of information exchanged under the policy.
- **Act in Good faith:** commit yourself to respect the content of your policy and don't pursue civil or criminal action against the participant complying with its terms.
- **Processing of personal data:** be clear about the obligations of the parties with regard to the processing of personal data.
- **Develop and deploy a solution** if possible and within a reasonable timing. Inform the participants as well.

- **Thank the participants**, even if they point out vulnerabilities. After all, they have tried to improve the security of your service. This is best done through a bug bounty programme, depending on the importance of the vulnerability. This form of policy is more attractive to potential participants and often more effective for your organisation. The reward can take different forms: financial, gift or simply public ranking of participants (e.g., a leader board).
- **Give participants the opportunity to publish** about the vulnerability. This is often a good reason for them to continue their researches. Publications about vulnerability (e.g. without mentioning your organisation) will help to improve the security of information systems.
- **Inform the CCB** (vulnerabilityreport@cert.be) and third parties (or their representative organisations) who are likely to be also affected by the vulnerability.

For participants

A CVDP offers a legal way of detecting and reporting vulnerabilities. This opportunity is based on an authorization, subject to certain conditions, and is based on mutual trust.

It is therefore important for you to carefully read the content of the CVDP before taking any action:

- **Comply with the conditions of the CVDP:** make sure you comply with the scope and terms of the CVDP.
- **Proportionality:** do not go beyond what is reasonable to prove the vulnerability. This is the common thread in all your actions.
  - If the vulnerability can be demonstrated on a small scale, there is no need to go any further.
  - Gather only the necessary evidence (downloads or screenshots) and preferably without personal data.
  - Do not disrupt the availability of the system, and do not exploit the vulnerability if this is not necessary to demonstrate and to document the vulnerability.
- **Confidentiality and security of the results of your researches:** do not share or disseminate any information regarding the discovered vulnerabilities with/to third parties, without the explicit authorization of the concerned organisation.

- **Be as comprehensive as possible** in your reporting. Also use timestamps to show that you acted as quickly as possible after the vulnerability was discovered: this will avoid any doubt about your intentions. Carry out upstream checks to confirm the existence of the vulnerability and identify any risks.
- **Continuous communication:** be patient and kind in your communication. The organisation may not know exactly how to respond appropriately to the vulnerability. It may also be that a vulnerability that has been reported several times without appearing to constitute a risk.
- **Act in good faith:** your actions must demonstrate that you have no fraudulent intent, no intent to harm, or will to use or cause damage to the visited system or its data.
- **Possible public disclosure:** always seek permission from the responsible organisation before any public disclosure on the vulnerability. Also allow a reasonable period of time (in coordination with the organisation) so that a solution can be developed and deployed. An organisation may always choose not to develop and deploy a solution, unless it is required to do so by law or contract. If you still believe that a solution should be developed, do not take any steps that would violate the CVDP and contact the CCB (vulnerabilityreport@cert.be) as coordinator.
- **Processing of personal data:** the purpose of a CVDP is not to intentionally process personal data, but it is possible that the participant may need to process such data
- in the course of their vulnerability research. In this case, please ensure that you comply with your obligations regarding the protection of personal data.
- **Do not ask for a reward** if it was not clearly predefined by the responsible organisation in its CVDP/bug bounty. Any request for a reward outside of the conditions defined in the CVDP may be considered as an unlawful extortion attempt.

If you happen to discover a vulnerability for an organisation that has not developed a CVDP, go no further. If the vulnerability is critical, contact a third parties coordinator such as a bug bounty platform or, by default, the CCB (vulnerabilityreport@cert.be). Any willing and unauthorised intrusion into a computer system remains punishable in the absence of a CVDP.

References

Guide to a Coordinated Vulnerability Disclosure Policy: Part I (Best practices), Centre for Cybersecurity Belgium (CCB), 2020 (www.ccb.belgium.be).

Guide to a Coordinated Vulnerability Disclosure Policy: Part II (Legal aspects), Centre for Cybersecurity Belgium (CCB), 2020 (www.ccb.belgium.be).

European Union Agency for Network and Information security (ENISA), Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure et Economics of Vulnerability Disclosure, 2018, www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

Software Engineering Institute, The CERT Guide to Coordinated Vulnerability Disclosure, 2013 (updated in 2019) https://vuls.cert.org/confluence/display/CVD

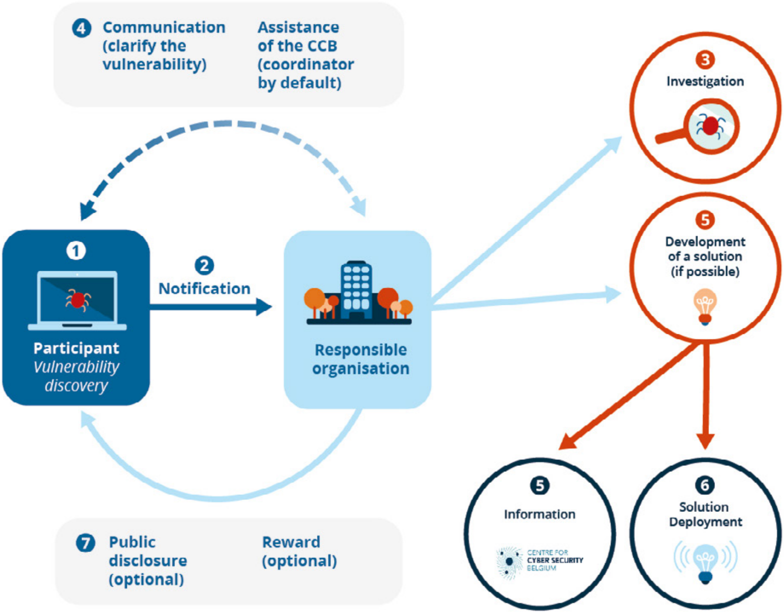
National Cyber Security Centre (NL), Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline), 2019, //english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline et Policy for arriving at a practice for Responsible Disclosure, 2013

CIO Platform Nederland - CEG Information Security, Coordinated Vulnerability Disclosure. Model Policy and Procedure, 2016, www.cio-platform.nl/en/publications et Coordinated Vulnerability Disclosure 1.4. Implementation guide, 2016, www.cio-platform.nl/en/publications

ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (www.iso.org/standard/72311.html).

ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

CVDP without coordinator

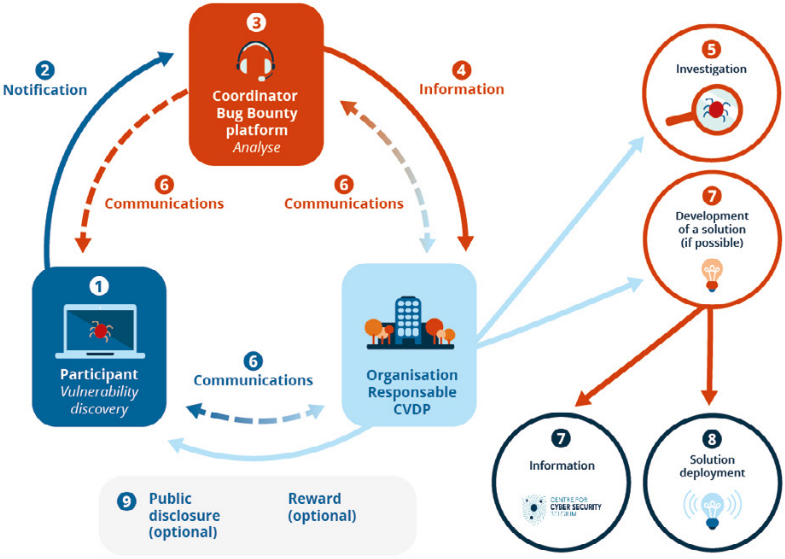

4 Communication (clarify the vulnerability)
Assistance of the CCB (coordinator by default)
1 Participant Vulnerability discovery
2 Notification
Responsible organisation
3 Investigation
5 Development of a solution (if possible)
5 Information
CENTRE FOR CYBER SECURITY BELGIUM
6 Solution Deployment
7 Public disclosure (optional)
Reward (optional)

1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation based on the CVDP details.
3. The responsible organisation analyses the vulnerablity.
4. Communication between the participant and the responsible organisation continues to clarify the vulnerability. assistance from the CCB (as coordinator by default) can be asked if there is a lack of communication in this process.

5 5 A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.

6. The responsible organisation deploys the solution to its users or customers.
7. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

CVDP with coordinator



1 Participant finds a vulnerability in the context of a CVDP.

2 Participant informs the responsible organisation through a coordinator, such as a bug bounty platform, based on the CVDP details.

3 The Coordinator analyses the vulnerablity.

4 After validation the coordinator will inform the responsible organisation.

5 The responsible organisation analyses the vulnerablity.

6 6 Communication between the participant and the responsible organisation continues to clarify the vulnerability, if desired through the coordinator.

7 7 A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.

8 The responsible organisation deploys the solution to its users or customers.

9 Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

This document and its annexes were drawn up by the Centre for Cyber Security Belgium (CCB). This federal public service was created by the Royal Decree of 10 October 2014 and is under the authority of the Prime Minister.

The CCB disclaims all liability in connection with the content of this document.

The information provided:
- is purely general in nature and does not aim to cover all specific situations;
- is not necessarily complete, accurate or up to date in all respects.

Prepress and printing
Central Printing Office of the House of Representatives

Brussels, October 2020

Responsible publisher:
Centre for Cyber Security Belgium
M. De Bruycker, Director
Wetstraat 18
1000 Brussels

D/2021/14828/003