Vulnerability reporting to the CCB

Every computer system or network may contain vulnerabilities. These vulnerabilities can be discovered by both well-intentioned people and by people with bad intentions. Apart from the existence of a coordinated vulnerability disclosure policy (CVD) or bug bounty, the fear of being sued often prevents well-intentioned people from looking for and reporting these vulnerabilities.

As part of the implementation of the national cybersecurity strategy, a legal framework has been adopted in Belgium to address this situation.

This framework allows any natural or legal person, acting without fraudulent or malicious intent, to investigate and report existing vulnerabilities in networks and information systems located in Belgium, provided that certain conditions are strictly respected (see detailed explanations).

One of these conditions is the two-step reporting of the discovered vulnerabilities to the Centre for Cybersecurity Belgium (CCB) according to the procedure established for this purpose below.

A. Background

The Centre for Cybersecurity Belgium (hereinafter, the "CCB"), in its capacity as a national CSIRT, can receive reports of potential vulnerabilities from natural or legal persons (see articles 22 and 23 of the Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security - hereafter the “NIS2 law”).

A vulnerability is defined in article 8, 15° of the NIS2 law as "a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat".

If an organisation has a coordinated vulnerability disclosure policy (hereafter “CVD”), researchers who discover a vulnerability should directly contact the concerned organisation and follow the requirements of its CVD. If difficulties arise (e.g. the responsible organisation fails to respond within a reasonable timeframe), if the potential vulnerability relates to a system, process or control that is not listed in the CVD, or the researcher feels that he is unable to comply with certain provisions of the CVD, he may always report a vulnerability to the CCB. When the vulnerability can affect other organisations that do not have a CVD, it should also be reported to the CCB.

The procedure for vulnerability reporting described below is quite distinct from the legal rules applicable to persons reporting violations of EU or national law based on information obtained in a professional context. Thus, the reporting of a violation of the legal rules for the protection of privacy

and personal data or the security of networks and information systems must comply with the legal rules provided for this purpose (see in particular the law of 28 November 2022 on the protection of persons who report breaches of Union law or national law detected within a legal entity in the private sector and the law of 8 December 2022 concerning reporting channels and the protection of whistleblowers of breaches of integrity in federal public sector organisations and within the integrated police), possibly combined with the rules of this procedure.

B. What are your obligations in the context of the search for and reporting of a vulnerability?

1° you do not act beyond what is necessary and proportionate to verify the existence of a vulnerability and to report it (see point C "proportionality and necessity of actions" below).

2° you must act without fraudulent intent or intent to harm.

You may not use your research for fraudulent purposes or with malicious intent. For example, you may not attempt to monetise the information discovered to the responsible organisation or to third parties (unless, of course, a reward or remuneration has been explicitly and previously agreed upon in the context of a pentest, bug bounty, agreement, etc.). Similarly, and without the contractual agreement of the responsible organisation, you may not use the discovered vulnerability for personal or third-party benefit.

When possible and to demonstrate your good intentions, make yourself known to the responsible organisation beforehand, during your research, for example by using a header or another identifiable parameter.

3° without undue delay and at the latest within 24 hours after the discovery of a potential vulnerability, you must address a simplified notification of the vulnerability to the organisation responsible and to the CCB, according to the procedure described in point D.

The notification of a vulnerability takes place in two stages: first a simplified notification within 24h, then a complete notification within 72h at the latest. The aim of the first notification is to inform the concerned organisation and the CCB that a potential vulnerability has been found. It contains an identification of the concerned systems and a simplified description of the potential vulnerability.

4° without undue delay and at the latest within 72 hours after the discovery of a potential vulnerability, you must address a full notification of the vulnerability to the organisation responsible and to the CCB, according to the procedure described in point D.

The full notification contains a detailed description of the vulnerability, including precise steps to reproduce it, as well as other technical information such as configuration details, operating system, tools used, etc.

When more than one person was involved in the research, then both the simplified as well as the complete notification may be made on behalf of several individuals who then assume collective responsibility. For convenience, multiple vulnerabilities involving the same responsible organisation can also be reported in a single simplified or complete notification. However, it is necessary to make separate notifications for each organisation concerned.

In order to establish the timeliness of your reports, it is recommended that you keep evidence of the actions taken (logging) with regard to the system, process or control concerned and that you communicate this information to the CCB at the time of the reports. Within the two deadlines, it is also recommended to do the reports prior to any active resistance by the responsible organisation (e.g., shutting down the ports) and/or any criminal investigation, to emphasize the timeliness of the reports.

5° you must not publicly disclose information about the discovered vulnerability without the agreement of the CCB (which will also take into account the position and context of the concerned organisation).

6° concerning the networks and information systems of some organisations (*) or judicial bodies, (and for information processed by or for them), you must, before starting your research, conclude a written vulnerability research agreement with the concerned service.

(*) SGRS/ADIV, VSSE, OCAM/OCAD, Ministry of defence, police services, Belgian diplomatic and consular missions outside the EU, Class I nuclear establishments, NCCN and CCB.

C. Proportionality and necessity of actions

Your actions must be strictly limited to what is necessary and proportionate to allow the discovery and the reporting of a vulnerability in a network or information system.

The following may be considered as such actions:

- unauthorised access or attempted access to a computer system (art. 550*bis* § 1 and 4 of the Criminal Code; art. 524 and 527 of the new Criminal Code);
- exceeding or attempting to exceed an authorization to access a computer system (art. 550*bis* § 2 and 4 of the Criminal Code; art. 525 and 527 of the new Criminal Code);
- taking over or copying computer data (art. 550*bis*, § 3 of the Criminal Code; art. 526 of the new Criminal Code);
- the development or possession of hacking tools (art. 550*bis*, § 5 of the Criminal Code; art. 528 of the new Criminal Code)

- possession, disclosure, use or disclosure of information obtained through unauthorised access, for example, information available on the Internet (art. 550*bis* § 7 of the Criminal Code; art. 530 of the new Criminal Code);
- introduction or modification of data in a computer system (art. 550*ter* of the Criminal Code; art. 531-533 of the new Criminal Code);
- interception or attempted interception of communications (art. 314*bis* of the of the Criminal Code; art. 342-346 of the new Criminal Code; and/or art. 145 of the law of 13 June 2005 of electronic communications);
- the violation of an obligation of professional secrecy or a contractual obligation of confidentiality (art. 458 of the Criminal Code; art. 352 of the new Criminal Code).

Your actions and research methods must remain necessary and proportionate regarding the objective of verifying the existence of a vulnerability in order to improve the security of the system, process or control concerned. The techniques used must therefore be strictly necessary and proportionate to the demonstration of a security flaw.

If the demonstration is possible on a small scale, you shall not extend your research further. The goal is not to use the vulnerability to examine how far one can penetrate a system, process, or control. Similarly, there is no justification for disrupting the availability of services provided by the affected equipment.

If not strictly necessary to demonstrate the existence of a vulnerability, the use and retention of data from the system, process, or control may not be performed. Similarly, all data collected should be deleted within a reasonable timeframe after the report. If it is necessary to keep this data for a longer period of time or if legal proceedings are in progress, you must ensure that this data is kept secure during this period.

The following may be considered as disproportionate and/or unnecessary actions:

- the installation of malicious software (malware): viruses, worms, trojan horses, or other;
- Distributed Denial Of Service (DDOS) attacks;
- Social engineering attacks;
- Phishing attacks;
- Spamming attacks;
- Password theft or brute force attacks;
- deletion of data from the computer system;
- the realization of a foreseeable damage to the visited system or its data;
- other offences from the Criminal Code not mentioned in the list above (e.g. burglary, theft, assault, etc.).

Finally, you should also take into account that if your vulnerability research is carried out on networks or information systems located in whole or in part outside the Belgian territory, the present reporting procedure will only protect you in Belgium and not in the other countries concerned.

D. How to report a security vulnerability to the National CSIRT (CCB)?

You must send the discovered information exclusively to the following e-mail address: **vulnerabilityreport[at]ccb.belgium.be**, with the following form.

The completed form must be sent to us in Word, ODT or PDF format, protected with a password, or in a password protected .zip file (to avoid possible blocking by our anti-virus filters).

The file must be a maximum of 7 MB.

SIMPLIFIED NOTIFICATION FORM

COMPLETE NOTIFICATION FORM

Whenever possible, we encourage you to use the following secure means of communication:

PGP Key ID: 0x31A9EA55

Type: RSA-4096 Key

Fingerprint: 8E98 3C10 BC8D 23BA EE1B 9CB9 670C A658 31A9 EA55

Protect the form with a password which can be communicated to us by e-mail.

Provide enough information to allow us to understand the vulnerability and resolve it as quickly as possible.

E. Consequences of the report

Provided that you strictly comply with all the conditions set out in point B, a cause of justification can be accepted in a limited way for the offences from articles 314*bis*, 458, 550*bis*, and 550*ter* of the Criminal Code, as well as article 145 of the law of 13 June 2005 on electronic communications.

When you report information on a potential vulnerability that you have become aware of in your professional context, you are not considered to have breached your obligation of professional secrecy and do not incur any liability whatsoever regarding the transmission of information necessary to report a potential vulnerability to the CCB.

Any other possible responsibility of the authors of the report arising from acts or omissions that are not necessary for the completion of the report procedure and that do not comply with all the

conditions listed in point B, remains intact. These acts or omissions continue to be punishable under criminal and civil law.

It is important to bear in mind that this legal protection is limited to the application of Belgian law and does not protect you against possible offences committed under the laws of other countries.

Finally, if you so request and if the conditions in point B are met, the CCB undertakes to respect the confidentiality of your identity.

F. Procedure

Upon receipt of a vulnerability report, the CCB will acknowledge receipt of the report to the reporter.

If an acknowledgement is not received within a reasonable period of time, or if the person has specific questions, he or she may, if necessary, contact vulnerabilitydisclosure[at]ccb.belgium.be.

The person reporting the vulnerability and the CCB undertake to make every effort to ensure continuous and effective communication in order to identify and address the vulnerability.

The CCB, in collaboration with the competent services of the Public Prosecutor's Office, will examine compliance with the conditions set out in points B and C.

G. Personal Data

In the course of your research and reporting of a vulnerability, you may come into contact with personal data.

The processing of personal data is broad in scope and includes the storage, modification, retrieval, consultation, use or disclosure of any information that may relate to an identified or identifiable natural person. The "identifiable" character of the person does not depend on the simple will of the data processor to identify the person but on the possibility to identify, directly or indirectly, the person with the help of these data (for example: an email address, identification number, online identifier, IP address or location data).

In this case, the reporter must make sure that he complies with his obligations regarding the protection of personal data as a data controller under the General Data Protection Regulation (GDPR).

Respecting the principles of necessity and proportionality, he must limit himself to the strict minimum possible processing of personal data and exclude their use for other purposes than demonstrating the existence of a vulnerability, demonstrating the reality of his actions, and communicating this information to the responsible organisation and to the CCB. Where the demonstration of a vulnerability is possible with a limited amount of personal data, not all accessible data need be processed or retained.

In particular, the reporter must ensure that the data he may have to process is stored with a level of security that is appropriate given the risks involved (preferably encrypted and anonymised) and that this data is deleted immediately after the processing ended (until the end of the reporting procedure or, in the event of a challenge or legal proceedings, until the end of the proceedings).

In case of a possible loss of personal data, which could create a risk for the rights and freedoms of the data subjects, the reporter must also inform the responsible organisation and the Data Protection Authority (DPA), as soon as possible and no later than 72 hours after becoming aware of it (see explanations and the required procedure on the DPA website).