Organisation for Economic Co-operation and Development

DSTI/CDEP/SDE(2021)9/FINAL

Unclassified English - Or. English

25 January 2023

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Security in the Digital Economy

Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities

JT03511220

Foreword

This document aims to provide policy makers with an overarching understanding of the co-ordination of digital security vulnerabilities in practice, while avoiding technical jargon and detailed considerations. It should be read in conjunction with the 2022 *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*.

This document was approved and declassified by the Committee on Digital Economy Policy (CDEP) at its 86th Session in May 2022, on the proposal of its Working Party on Security in the Digital Economy (SDE). It was prepared for publication by the OECD Secretariat.

This document was drafted by Laurent Bernat, of the OECD Secretariat, with valuable input from SDE and CDEP delegates, as well as support and feedback from experts involved in OECD analytical work on digital security vulnerabilities initiated in 2020, which led to the development of the *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*.

The *OECD Policy Framework on Digital Security: cybersecurity for prosperity* provides a broad presentation of OECD standards and approach to digital security, and explains how the treatment of digital security vulnerabilities fits within this broader picture.

More information about OECD work on digital security is available at: https://oe.cd/security.

Table of contents

Introduction

The following good practice guidance aims at supporting the implementation of the OECD *Recommendation on the treatment of digital security vulnerabilities* ("Vulnerabilities Recommendation")[1].

The treatment of digital security vulnerabilities covers the discovery, handling (by code owners), management (by system owners) and disclosure of vulnerabilities by vulnerability researchers. This document focuses on vulnerability co-ordination, i.e. the relationships between vulnerability owners and vulnerability researchers, which is a specific aspect of vulnerability treatment.

This good practice guidance aims to provide policy makers with an overarching understanding of the co-ordination of digital security vulnerabilities in practice, while avoiding technical jargon and detailed considerations. It may also help technical security experts to communicate with policy makers and non-technical experts in their organisation such as CEOs, board members, communication, and legal departments, etc. This document is expected to be sufficiently consistent with technical standards and other guides targeting technical experts in this area, does not aim to replace them, but rather helps raise awareness about their existence and the need for practitioners to use them.

Therefore, this document is formulated at a relatively high level and does not cover all aspects of vulnerability co-ordination. Examples of areas that are not covered include guidance for vulnerability researchers[2], in particular, about the conditions and modalities for publicly disclosing vulnerabilities when co-ordination fails; details such as the threshold beyond which a vulnerability researcher should consider that a vulnerability owner is unresponsive, or is too slow to develop mitigation; how to publish vulnerability disclosure policies; how to determine what information should be publicly disclosed; details of multi-"vendors" or multi-party vulnerability co-ordination, etc.

These important issues, and many others discussed in OECD analytical work[3] raise complex questions that deserve further discussions among stakeholders prior to being reflected in a document targeting primarily policy makers. Nevertheless, this document may be revised in the future by the Committee on Digital Economy Policy (CDEP) and its Working Party on Security in the Digital Economy (WPSDE) to reflect progress made in this area and continue to best inform policy makers.

It is expected that the incompleteness of this good practice guidance will stimulate policy makers and all stakeholders to continue their dialogue and fill the missing parts.

The good practice guidance builds upon multiple existing guides and documents on co-ordinated vulnerability disclosure listed in the References section.

Box 1 provides definitions of key terms included in this document.

---

1 OECD (2022), *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*, OECD/LEGAL/0482, OECD, Paris.

2 The Vulnerabilities Recommendation recommends that Adherents cooperate with all stakeholders at the international level to develop such guidance. See IX.2.e.

3 OECD (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en. See also the policy note on this subject at: www.oecd.org/digital/encouraging-vulnerability-treatment.pdf.

Box 1. Terminology

- **Digital security vulnerabilities,** or "vulnerabilities", refers to technical weaknesses in products and information systems that can be exploited to damage economic and social activities. They include:
  - *Code vulnerabilities*, which are located in the code of products; and
  - *System vulnerabilities*, which affect information systems and include primarily misconfigurations and the non-application of products' security updates, patches or other mitigations.
- **Vulnerability researchers** refers to individuals or organisations who identify potential code or system vulnerabilities with the intention to reduce related security risk. They are sometimes also called "ethical hackers", or "white hat hackers".
- **Vulnerability owners** refers to stakeholders with responsibility to mitigate a vulnerability they are aware of. They include **code owners** (also known as "vendors"), who are responsible to develop and maintain a layer of code embedded in a product, including through vulnerability handling (e.g. developing a patch and distributing it, for example through a security update). Code owners form the first line of defense against malicious actors. They are often called vendors, suppliers, developers, maintainers, or manufacturers. Vulnerability owners also include **system owners**, who are responsible to mitigate system vulnerabilities, including through vulnerability management (e.g. applying patches and security updates). System owners are the second line of defense. The combination of these first and second lines of defense reduces security risk related to the possible exploitation of vulnerabilities.
- **Vulnerability handling** refers to the risk-based processes followed by code owners to verify information about a newly discovered vulnerability and resolve that vulnerability by developing and disseminating the appropriate mitigation to affected system owners (e.g. security update, patch, workaround).
- **Vulnerability management** refers to the ongoing risk-based processes enabling a system owner to know if vulnerabilities are present within its digital ecosystem and take appropriate risk management decisions and actions to mitigate them.
- **Vulnerability reporters** refers to the individuals or organisations who report a vulnerability. They are sometimes called "finders" and include vulnerability researchers as well as other parties such as co-ordinators, users of the product or information system, penetration testers, etc.
- **Vulnerability treatment** refers to the overarching process encompassing vulnerability discovery, handling (by code owners), management (by system owners) and disclosure. It includes all the actions taken to discover vulnerabilities, and:
  - *For code vulnerabilities*, to develop a mitigation (e.g. a patch, security update, workaround), distribute it to a product's users, and disclose the vulnerability to the public or the security community; and
  - *For system vulnerabilities*, to apply an existing mitigation or remediate the misconfiguration;
- **Co-ordinated vulnerability disclosure** (CVD) refers to the process through which vulnerability owners and researchers work co-operatively in finding solutions that reduce the risk associated with a vulnerability. CVD is part of vulnerability treatment.

Source: *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*.

I. Sharing a common understanding

1. All stakeholders share the following basic common understanding:
    a. All products that include code may also include vulnerabilities; all products might appear free of vulnerabilities at a certain point or in a certain context but may become vulnerable later or when the context changes; all information systems may include vulnerabilities related to misconfigurations and the non-application of products' security updates and patches.
    b. These vulnerabilities may represent a danger because threat actors can exploit them and create damages for all stakeholders, and, in some cases, for the economy and society as a whole. Digital security attacks affect economic and social prosperity and human rights, undermine trust in the digital economy, reduce the potential benefits from digital transformation, threaten the security, privacy and safety of individuals, and the delivery of activities that are critical to the functioning of our economies and societies, such as health care, water treatment, energy distribution and elections.
    c. Not all vulnerabilities can be eliminated; however, it is possible to remediate or at least mitigate many of them, and priority should be given to those vulnerabilities that pose the greatest risk.
    d. Co-ordinated Vulnerability Disclosure (CVD) is a process whereby stakeholders who own the responsibility to eliminate vulnerabilities in products or systems (vulnerability owners) and vulnerability researchers who have found a vulnerability in these products or systems combine efforts and work collaboratively towards the common goal of increasing the security of (or reducing digital security risk to) all stakeholders. A key goal of CVD is to reduce the adversaries' advantage while a vulnerability is being fixed. CVD is an important part of vulnerability treatment.
    e. There is no one-size-fits-all in vulnerability reporting and disclosure. Stakeholders agree to follow good practices and policies while recognising that they reflect intended paths for general cases and may not be optimal in all circumstances. Therefore, they work co-operatively both to address each situation according to good practice, and to determine the best approach when good practice is not the best solution to reduce risk in specific cases.
    f. Effective vulnerability disclosure is as much a matter of trust between humans as a technical challenge.

II. Taking responsibility

2. Vulnerability owners and vulnerability researchers work together to treat vulnerabilities and share information with other stakeholders. They share the common goal to minimise stakeholders' window of exposure to the exploitation of vulnerabilities by malicious actors. While most often time is of the essence, stakeholders co-operate to ensure that remediation or mitigation measures are sufficiently tested before being disseminated, to minimise the likelihood of creating new vulnerabilities and other negative side effects.

II.1. Vulnerability owners

3. Vulnerability owners:

    a. Are responsible for the security of the system they operate or product they developed, and to address related vulnerabilities according to the risk they raise to themselves, users, third parties and the economy and society as a whole;

    b. Are prepared to receive and address solicited and unsolicited vulnerability reports as part of their normal duty of care and responsibility, and to co-ordinate vulnerability disclosure, according to their capacity (e.g. size, resources, number of reports, etc.);

    c. Publish and implement Vulnerability Disclosure Policy (VDP) (see below IV).

    d. Treat all vulnerability reports with equal attention and respect, provide informative and proactive feedback to the vulnerability researcher about vulnerability reproduction, remediation or mitigation, and disclosure; acknowledge and, where possible, honor the work of the vulnerability researcher publicly (in press release, security bulletin, and in the vulnerability advisories); support vulnerability researchers in case of wrongful legal proceedings against them;

4. More specifically:

    a. *Code owners:*

        - Handle any known vulnerabilities as part of the basic support of their products and secure product development lifecycle,

        - Inform and co-ordinate remediation efforts with upstream and downstream stakeholders when the code vulnerability is embedded in third-party products (e.g. multi-party or supply chain co-ordination).

    b. *System owners* maintain systematic vulnerability management cycles to identify:

        - configuration errors and ensure that they are rapidly corrected,

        - which products they use have known vulnerabilities and ensure that the latest security update or other remediation or mitigation measures (e.g. security updates, patches, workarounds) are applied to them as rapidly as possible, taking into account the business and technical risk inherent to vulnerability management.

II.2. Vulnerability researchers

5. Vulnerability researchers are responsible for their own actions, including for the way in which they discover, report and disclose a vulnerability. They do not do more than what is necessary to demonstrate a vulnerability, or how to mitigate it.

6. Vulnerability researchers:

    a. Report the vulnerability to the vulnerability owner first and as soon as possible after its discovery, or contact a co-ordinator (see below IV) if they cannot reach the vulnerability owner, using sufficiently secure means of communication in all cases;

    b. Provide clear documentation and artefacts to support the reproduction process whereby the vulnerability owner ensures that the vulnerability exists, and understands how an attacker could exploit it;

c. Read the conditions set by a vulnerability owner in its VDP, make the best effort to follow them and, in case of disagreement with the conditions, or in absence of a VDP, contact a co-ordinator and follow good practice for CVD;

d. Give the vulnerability owner a reasonable amount of time to process the vulnerability report;

e. Do not require a reward as a condition to report a vulnerability. The initiative for granting a reward lies with the vulnerability owner.

III. Creating sustainable trust

7. All CVD Stakeholders build and maintain trust, including by:

   a. **Presuming benevolence**, good intent, and good will from other CVD stakeholders.

   b. Clearly **communicating intentions** and making a good faith effort to understand respective expectations and perspectives.

   c. Maintaining **continual or frequent communication** characterised by quality, mutual respect, patience, and transparency.

   d. Adequately **handling sensitive information** and using sufficiently secure communication channels.

   e. Being **transparent** about expected processes and milestones (timelines), including the remediation and disclosure process.

   f. **Reducing uncertainty**, surprise, and potential for dissatisfaction for other CVD stakeholders.

   g. **Negotiating expectations** and timelines if standard processes are not appropriate.

   h. **Avoiding legal or other coercive pressure or threat**, actual or perceived, as well as escalation, including legal action, to any extent possible, to prevent a chilling effect on desired vulnerability research.

IV. Seeking the assistance of a co-ordinator

8. Stakeholders who face difficulties in establishing or carrying out a CVD process request support from a trusted third-party co-ordinator. The co-ordinator is often a Computer Security Incident Response Team (CSIRT) or a Product Security Incident Response Team (PSIRT).

9. A co-ordinator can for example help connect stakeholders, provide additional technical analysis and other support, particularly when there is disagreement or dissatisfaction among the parties, or in case of complex reports such as those involving multiple vulnerability owners (multi-party / supply chain co-ordination). The co-ordinator can also help address cross-border challenges. In addition, some co-ordinators can help share knowledge about the vulnerability within the technical security community, for example by publishing security advisories.

V. Adopting a Vulnerability Disclosure Policy

10. At a minimum, a VDP contains a point of contact for vulnerability researchers to report vulnerabilities securely.

11. A VDP is based upon the following principles:

    a. **Clarity:** a VDP is public, uses plain, easily understood terms, without jargon or ambiguous language. It does not evolve frequently and, when it does, it tracks, explains, and documents changes made.

    b. **Scope:** a VDP captures the organisation's intent accurately, clearly, and specifically; and defines the scope of the vulnerability disclosure programme, which is proportionate to the vulnerability owner's capacity to effectively process reports.

    c. **Rules of the game:** a VDP describes authorised and unauthorised conduct; explains the consequences of complying and not complying with the policy, including legal protections offered to compliant vulnerability researchers; defines conditions under which the vulnerability owner agrees not to initiate or support legal action against researchers; and encourages participants to contact the organisation for clarification before engaging in conduct that may be inconsistent with or unaddressed by the policy.

    d. **Transparency:** a VDP explains how reported vulnerabilities will be processed, indicates clear modalities for secure and possibly anonymous communication, clarifies expectations with respect to acknowledgments and rewards (as appropriate), timelines, response times and follow-up communications during the process, confidentiality, and for code vulnerabilities: expectations related to the development of a remediation, its dissemination and public disclosure.

    e. **Facilitation:** a VDP highlights the possibility to contact a co-ordinator to facilitate the process.

VI. Establishing appropriate internal processes for CVD

12. Vulnerability owners approach CVD as a complement rather than as a substitute to or replacement for other security measures.

13. When engaging in CVD, vulnerability owners:

    a. **Allocate sufficient internal resources**, define clear roles and responsibilities for handling vulnerability analysis and communication tasks, and scale their vulnerability disclosure programme progressively, according to their learning curve, maturity, and internal capacity to process reports. To do so, they can use metrics such as reported vulnerabilities, false-positive reports, time taken to communicate with the researchers, and time to mitigate discovered vulnerabilities;

    b. **Co-ordinate internally** with the business, legal and communications teams and integrate CVD as part of business decision making processes rather than keeping it as an isolated technical process;

    c. **Establish a strong foundation of tested processes and relationships,** following existing international standards, guidance documents and best practice, to ensure predictable response and relationships with vulnerability researchers and third parties, to operate a clear, publicly known, regularly monitored, and adequately

secure intake mechanism, and appropriate communication channels with vulnerability researchers;

d. **Consider third parties' interests**. For example, if the reported vulnerability is located in a third-party component of a product, this product's manufacturer extends the CVD process to the component's code owner;

e. **Follow international technical standards**, where appropriate, for example to represent and exchange vulnerability information in order to facilitate the use of automated tools by third parties;

f. **Anticipate challenges**, for example, by deciding, in advance of launching the CVD programme, how it will handle accidental, good faith violations of the VDP, as well as intentional, malicious violations;

g. **Establish a cycle of improvement**, by capturing lessons learned from vulnerability reports to enable improvement of their overall security practices, including the CVD process itself.

References

The above overview of good practice is based on an analysis of the following documents (in chronological order) as well as input from OECD delegations and experts:

1. Christey Steve, Wysopal Chris (2002), Responsible Vulnerability Disclosure Process.
2. US-CERT (2012), Common Industrial Control System Vulnerability Disclosure Framework.
3. ENISA (2016), Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations.
4. Rabobank, CIO Platform Nederland (2016), Manifesto on Co-ordinated Responsibility Disclosure.
5. NTIA Safety Working Group (2016), "Early Stage" Co-ordinated Vulnerability Disclosure Template. Version 1.1.
6. Householder D., Wassermann G., Manion A., King C., (2017), The CERT® Guide to Co-ordinated Vulnerability Disclosure. CMU/SEI-2017-SR-022.
7. FIRST (2017), Guidelines and Practices for Multi-Party Vulnerability Co-ordination and Disclosure, v 1.0.
8. US Department of Justice (2017), A Framework for a Vulnerability Disclosure Program for Online Systems, version 1.0.
9. Dutch National Cyber Security Centre (2018), Co-ordinated Vulnerability Disclosure: The Guideline.
10. Cybersecurity Coalition (2019), Policy Priorities for Co-ordinated Vulnerability Disclosure and Handling.
11. Center for Cybersecurity Policy and Law (2019), Improving Hardware Component Vulnerability Disclosure.
12. Business Software Alliance (BSA) (2019), Guiding Principles for Co-ordinated Vulnerability Disclosure.
13. UK National Cybersecurity Center (NCSC-UK) (2020), Vulnerability Disclosure Toolkit.
14. Cybersecurity and Infrastructure Security Agency (CISA) (2020), Binding Operational Directive 20-01. Develop and Publish a Vulnerability Disclosure Policy.