TECHNICAL REPORT

ISO/IEC TR 5895

First edition
2022-06

Cybersecurity — Multi-party coordinated vulnerability disclosure and handling

Cybersécurité — Divulgation et traitement de vulnérabilité coordonnée entre plusieurs parties

Reference number
ISO/IEC TR 5895:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives orwww.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Remediation of vulnerabilities in modern technology systems can vary and depend on the nature of the vulnerable component. Certain vulnerability handling efforts can require multiple ecosystem players taking action at multiple and interdependent layers within a given information and communication technology (ICT) system. Mitigation can necessitate the engagement of the broad ecosystem of stakeholders to develop, test and deploy mitigations in a manner geared to incentivize adoption by end users.

For example, a vulnerability in a widely used software library (protocol) can entail action by different ecosystem players as part of the remediation effort. As another example, a remediation development and testing for a vulnerability in a hardware component can depend on an operating system running on the hardware, and require different actions from different operating system providers. Due to these considerations, multiple vendors need to participate in remediation efforts involving certain vulnerabilities.

Yet vulnerability disclosure and handling processes as described in ISO/IEC 29147 and ISO/IEC 30111 primarily focus on processes involving one reporter and one vendor. Further discussion and considerations are necessary to explain how ISO/IEC 29147 and ISO/IEC 30111 practices apply in the context of multi-party coordinated vulnerability handling and disclosure (MPCVD).

ISO/IEC 29147 and ISO/IEC 30111:2019, Clause 8 briefly and generally address the complex situation of MPCVD, where a broader collaboration within the ecosystem is needed to identify and validate vulnerabilities, develop and test mitigations and finally make them available for end users. ISO/IEC 30111 refers to these situations as "cases where vendors can share vulnerability information in order to resolve the issue that involves components from multiple vendors" and provide five examples of such situations or reasons:

a) A vulnerability which was reported that affects a specific piece of software, but is caused by an issue in an underlying operating system or hardware.

b) Vulnerabilities in various product implementations of a flawed standard functional specification or in published algorithms.

c) Vulnerabilities that are naturally induced by so far widely accepted development methodology.

d) Vulnerabilities in commonly used libraries.

e) Vulnerabilities in software components that lack a current maintainer.

The MPCVD effort for a vulnerability in a technology owned and manufactured by the vendor leading the process – the coordinating vendor, or mitigating vendor manages and leads the coordination effort. The mitigating vendor (example a) above) can entail different processes from one in which a broader collaboration is needed and there is no one distinct vendor of the technology (e.g. protocol-level vulnerabilities) (examples b) to e) above). These examples include both vendor-coordinated MPCVD and non-owner MPCVD. Recognizing MPCVD can raise unique considerations for vulnerability handling given the technical and coordination complexities. Several documents have been published to share norms and best practices in this evolving area. These best practices continue to be developed, iterated and improved as new challenges arise. This document builds upon these sources and refers to them.

The audience for this document includes, among others, the participants of the MPCVD process such as vendors (defined in ISO/IEC 29147:2018, 3.4), maintainers, producers, developers, manufacturers, suppliers[1)], installers, or providers of a product or service, coordinators (including public coordinators), reporters (e.g. security researchers), and users of information technology products and services.

1) By way of example, when the open source maintainer is leading the coordination effort in the non-owner MPCVD case or as "dependent vendor", a "vendor" can also include open-source software maintainers who develop and distribute code.

Cybersecurity — Multi-party coordinated vulnerability disclosure and handling

1 Scope

This document clarifies and increases the application and implementation of ISO/IEC 30111 and ISO/IEC 29147 in multi-party coordinated vulnerability disclosure (MPCVD) settings, including the evolving commonly adopted practices in this area, by articulating:

— The MPCVD life cycle and application of coordinated vulnerability disclosure (CVD) stages (preparation, receipt, verification, remediation[2)] development, release, post-release) in MPCVD settings.

— Stakeholders involved in MPCVD include users, vendors (coordinating, mitigating, and dependent vendors), reporters, and non-vendor coordinators (entities defined in ISO/IEC 29147 and ISO/IEC 30111).

— The exchange of information between stakeholders during the vulnerability handling and disclosure process in a MPCVD settings.

Clarifying the application of ISO/IEC 30111 and ISO/IEC 29147 in MPCVD settings illustrates the benefits of vulnerability disclosure processes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

ISO/IEC 30111:2019, *Information technology — Security techniques — Vulnerability handling processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 30111 and ISO/IEC 29147 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Concepts

4.1 General

MPCVD processes are generally based on two concepts: (1) when security vulnerabilities arise, vendors work quickly, collaboratively and effectively to mitigate the vulnerabilities, and (2) all involved parties (which includes the various entities working on the mitigations and the reporters who discovered

2) Remediation is a defined term used in ISO/IEC 30111 and ISO/IEC 29147. This document uses the term "remediation" and verb “remediate” in the context of this definition.

or reported the vulnerabilities, if applicable) simultaneously take steps to decrease the risk that information about the vulnerabilities becomes publicly available before mitigations are available, in order to protect end users.

The implication for MPCVD is that processes can take a longer period than in other environments (such as traditional CVD processes involving one entity in the handling processes) to fully develop, validate and deploy mitigations while information concerning the vulnerability is simultaneously kept in confidence (often termed, "embargo") to protect end users from potential exploitation. The embargo period is during the vulnerability handling process but prior to public disclosure, during which information concerning the vulnerability is kept in confidence and only shared with entities necessary for the remediation development process. Similar to other CVD processes, MPCVD processes rely on the notion that information concerning the vulnerability is generally publicly disclosed only after mitigations are available to end users.

The MPCVD effort for a vulnerability in a technology owned and manufactured by the vendor leading the process can entail different processes from one in which a broader collaboration is needed and there is no one distinct vendor of the technology (e.g. protocol-level vulnerabilities).

MPCVD processes, generally include a higher level of complexity and involvement by a wide range of stakeholders in the various stages of CVD, as shown in Figure 1. For example, generally the MPCVD process cases where there is a security vulnerability affecting hardware often need broader collaboration within the ecosystem. Mitigation of vulnerabilities in hardware can require acting at multiple and interdependent layers within a given computing system. This, in turn, can necessitate the engagement of a larger number of third-party participants to develop, test and deploy mitigations in a manner most likely to incentivize adoption by end users. Mitigation of a hardware vulnerability can require updates to processor microcode and/or firmware, as well as interdependent updates to the operating system software or other system software. These updates are then delivered to end-users through multiple channels, including operating system (OS) and virtualization vendors, cloud service providers (CSP) or original equipment system manufacturers (OEM). Hardware manufacturers often do not have a means to unilaterally deliver mitigations without the direct participation of such entities in the global supply chain.

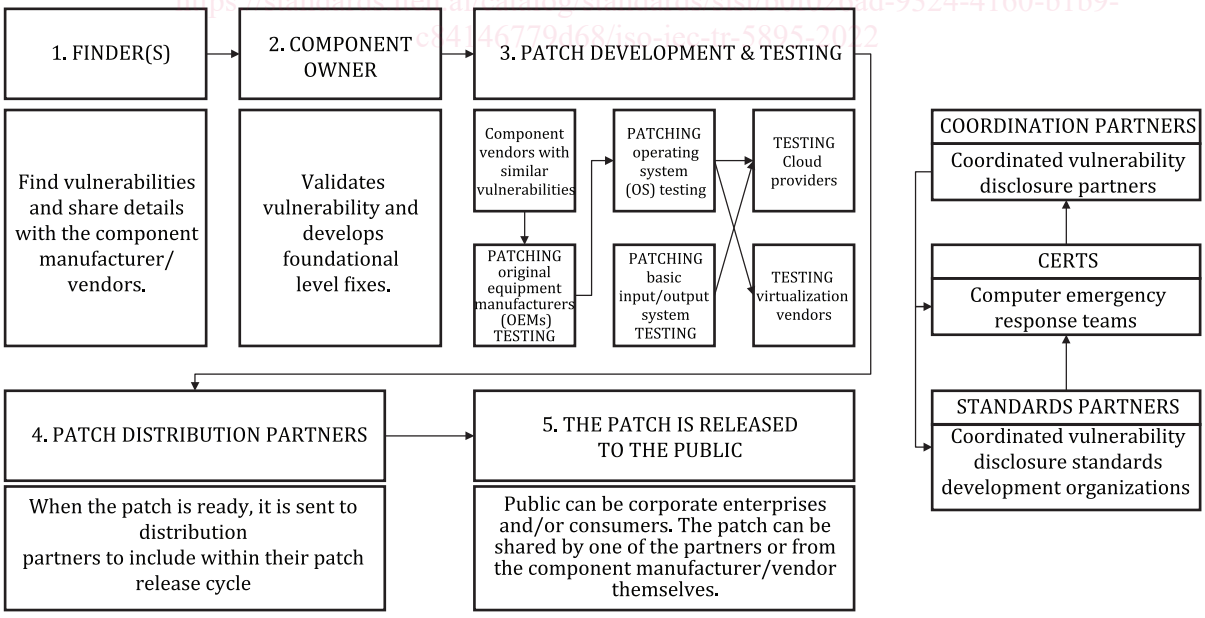

Figure 1 — Example of vendor-coordinator led MPCVD process — coordinated vulnerability disclosure in hardware systems[1]

4.2 Relationship with other International Standards

4.2.1 ISO/IEC 29147 - Vulnerability disclosure

ISO/IEC 29147 is used in conjunction with this document. The relationship between the two documents is shown in Figure 2.

ISO/IEC 29147 provides guidelines for vendors on how to process and remediate potential vulnerabilities reported by internal or external individuals or organizations. While this document deals with the interface between multiple vendors, layers of customers, cross manufacturer collaborative mitigation strategies and multiple reporters, ISO/IEC 29147 provides guidelines for vendors to include in their normal business processes when receiving reports about potential vulnerabilities from external individuals or organizations and when distributing vulnerability remediation information to affected users. This document clarifies the application of these disclosure-related processes in MPCVD settings.

4.2.2 ISO/IEC 30111 - Vulnerability handling processes

ISO/IEC 30111 is used in conjunction with this document. The relationship between the two documents is shown in Figure 2.

ISO/IEC 30111 gives guidelines on how to investigate, process and resolve potential vulnerability reports. While this document deals with the interface between multiple vendors, layers of customers, cross manufacturer collaborative mitigation strategies and multiple reporters, ISO/IEC 30111 deals with internal vendor processes including the triage, investigation and remediation of vulnerabilities, whether the source of the report is external to the vendor or from within the vendor's own security, development or testing teams. This document clarifies the application of these handling-related processes in MPCVD settings.

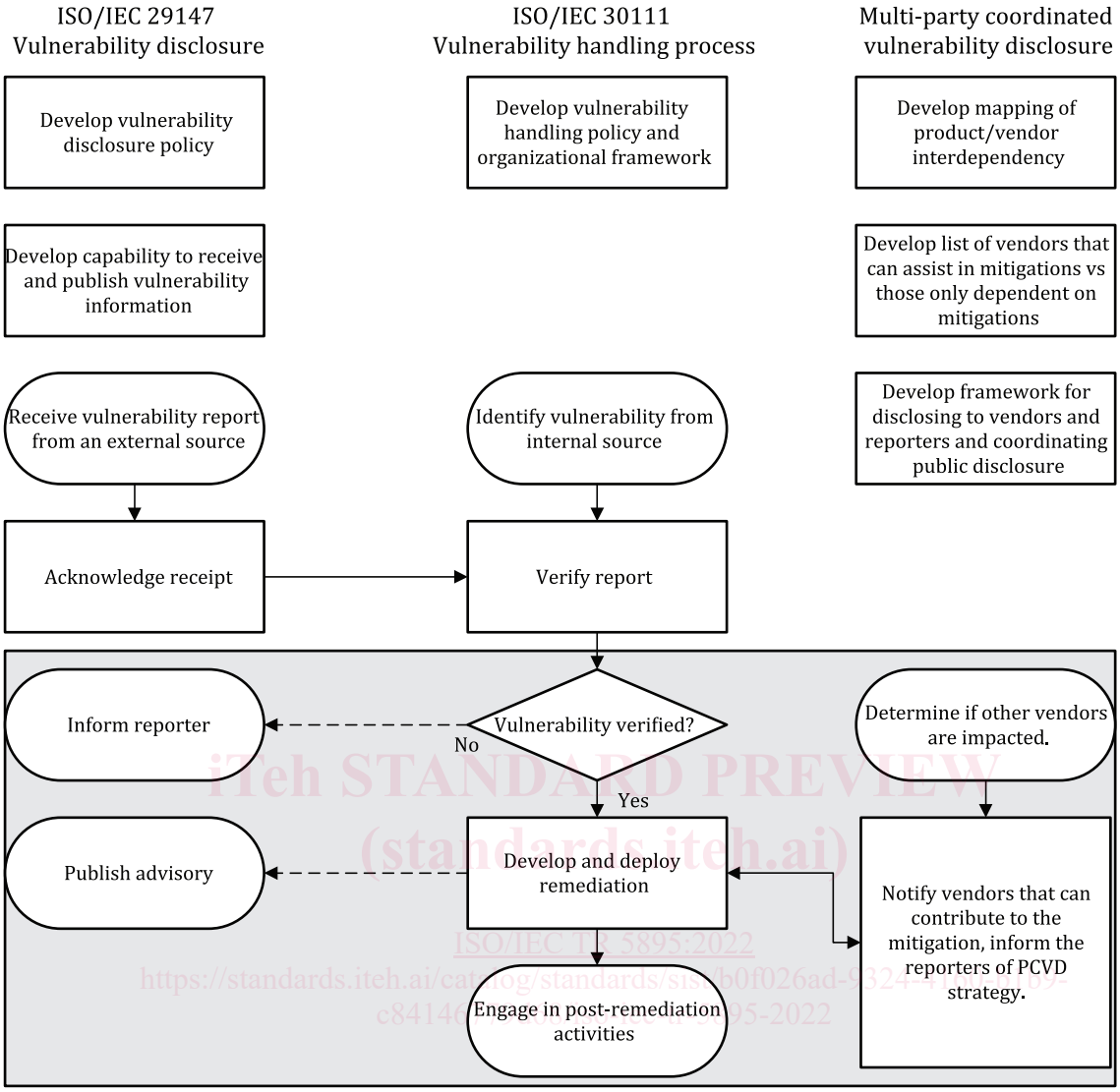

Figure 2 — The relationship between ISO/IEC 29147 and ISO/IEC 30111 with respect to MPCVD

4.2.3 Risk reduction effectiveness

Similar to the concept of the impact of successful exploitation referred to in ISO/IEC 30111, risk reduction effectiveness is an element that can be considered in the context of MPCVD. The risk reduction effectiveness measures the effectiveness of public disclosure and associated mitigation and/or remediation against the total cost to society if the vulnerability is exploited. Risk reduction effectiveness is a function that is affected by a variety of uncertainties, such as:

— Malicious attackers gaining knowledge about vulnerabilities from disclosed vulnerability and mitigation information, increasing exploitation risk.

— Delayed delivery and/or publication of mitigations and vulnerabilities because there are multiple contributors (e.g. vendors and open source maintainers) that need to be engaged or added to the engagement.

— The need for collaboration between vendors across the supply chain, either vertically (vendors participating and supplying various components to the final product) or horizontally (vulnerability-affected vendors scattered in a supply chain) can increase the coordination period and introduce unpredictable variables along the process that can impact expectations around timeline/embargo periods.

MPCVD increases the summation of the risk reduction effectiveness. In other words, a primary purpose of MPCVD is to reduce the potential harm to users and the public by increasing the effective collaborations in the relevant CVD stages prior the public release, which includes increasing the completeness and effectiveness of the proposed remediation while incentivizing its adoption by end users at disclosure.

5 MPCVD scenarios

5.1 General

Clause 5 provides common scenarios of MPCVD in the scope of this document.

5.2 MPCVD led by the vendor-coordinator (the owner of the technology developed) – the "mitigating vendor"

In the MPCVD case of the vendor-coordinator (e.g. hardware), there is generally a clear owner/developer of the underlying vulnerable technology who is typically best-situated to lead the coordination effort as the most technically knowledgeable of the product and component supply chain. For example, software companies, including operating systems and firmware vendors, and virtualization vendors can be integral to the process of developing and testing a mitigation for a hardware-based vulnerability (taking part in the handling processes), which are coordinated and led by the hardware manufacturer, as the mitigating vendor. In different MPCVD settings where there is no clear owner of the technology/ manufacturer best-situated to lead the coordination efforts (for example, in certain protocol-level vulnerabilities), a different entity can act as a coordinator, leading the coordination effort.

5.3 MPCVD process in non-owner cases

In the case where there is no clear owner of the technology who is typically best-situated to lead the remediation development and other CVD processes, a different "coordinator" (see ISO/IEC 29147:2018, 5.5.5) can act as the entity or intermediary leading the MPCVD process.

6 MPCVD stakeholders

6.1 General

Clause 6 describes significant stakeholder roles beyond those found in ISO/IEC 29147.

6.2 Vendor

ISO/IEC 29147 provides the definition of a vendor. Vendors are described as individuals or organizations who create or provide software products, including manufacturers, developers, or distributors. MPCVD allows for vendors to take on the following roles. Additionally, vendors can also act as coordinators depending on the issue.

6.2.1 Mitigating vendor

Mitigating vendors lead the MPCVD process, including facilitating the coordination with dependent vendors (e.g. disseminating the proposed mitigation developed by the mitigating vendor to dependent vendors and coordinating its testing in various environments). This can include coordinating the dependent vendor contribution to the remediation development (e.g. if independent mitigations developed by the dependent vendor need to be applied along with the proposed remediation to fully protect against a specific security vulnerability and subsequently released together).