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.

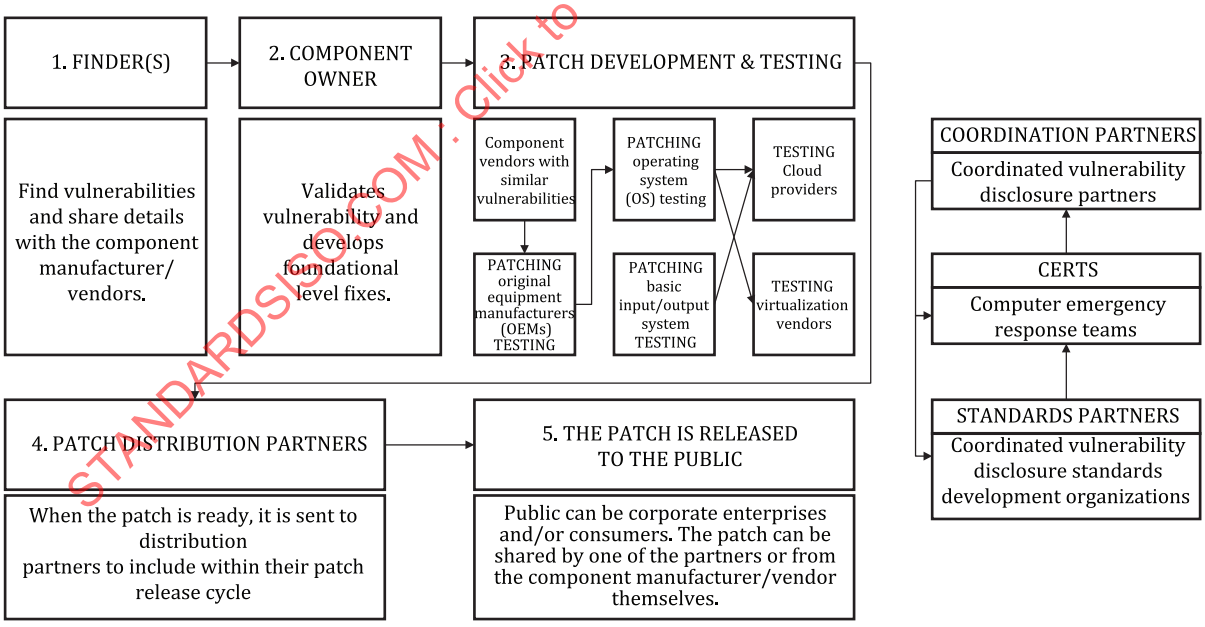

Figure 1 — Example of vendor-coordinator led MPCVD process — coordinated vulnerability disclosure in hardware systems[1]

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.

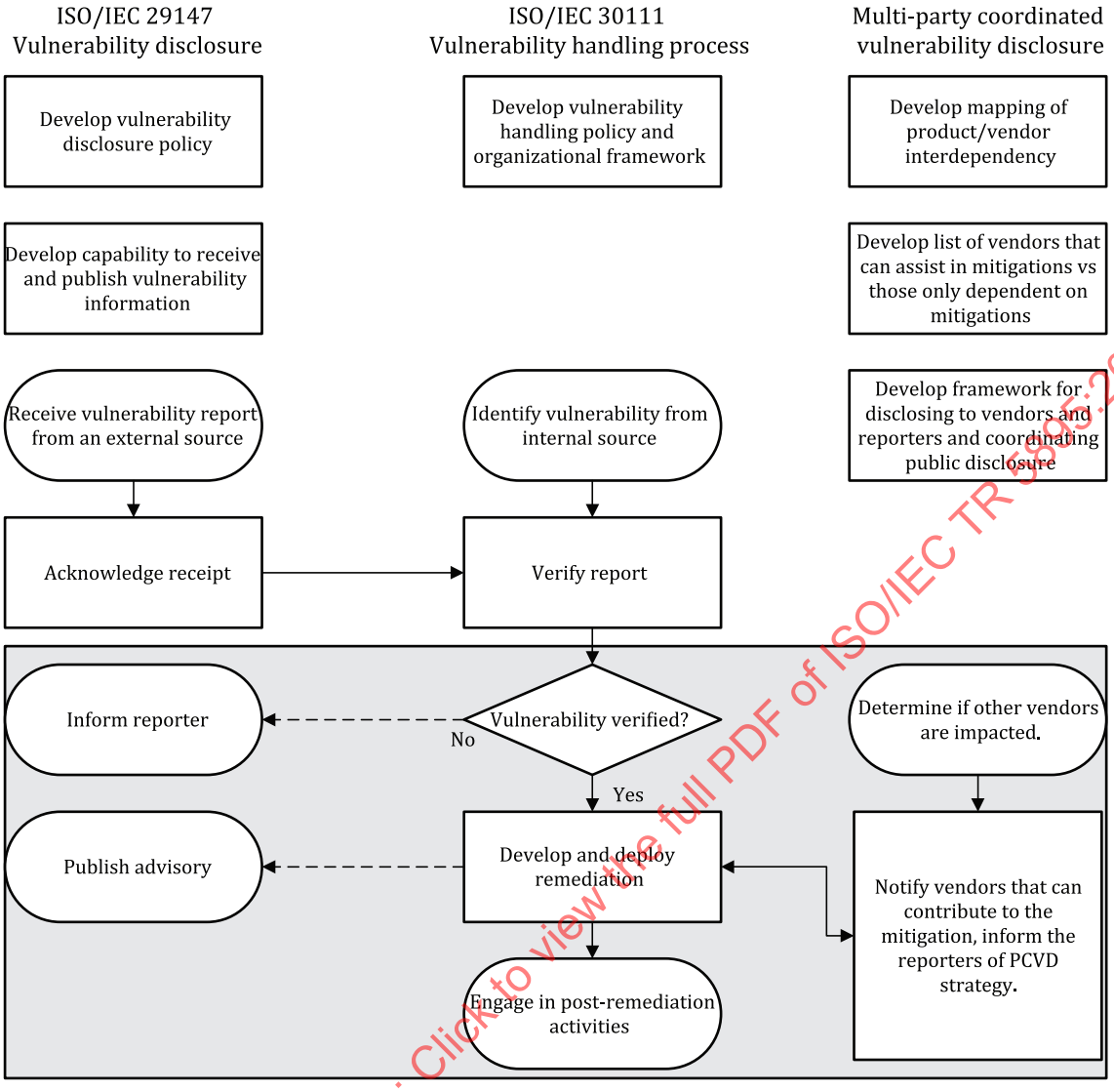

Figure 2 — The relationship between ISO/IEC 29147 and ISO/IEC 30111 with respect to MPCVD

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).

6.2.2 Dependent vendor

ISO/IEC 29147 provides the definition of a dependent vendor. Dependent vendors are vendors taking part in the MPCVD process due to their necessity to take action as part of the remediation development, validation, testing and release. They take part in the coordination effort and MPCVD process led by the mitigating vendor. Dependent vendors are typically downstream of mitigating vendors.

6.2.3 Mitigating vendor and coordination

Mitigating vendors often coordinate vulnerability and remediation details with dependent vendors. The mitigating vendor, acting as a coordinator, can act as the intermediary between the reporter and other dependent vendors. The mitigating vendor in this respect takes on a similar role as a non-vendor coordinator. More information on coordinators can be found in ISO/IEC 29147.

6.3 Non-vendor coordinator

In addition to the description of a coordinator in ISO/IEC 29147, there are other considerations for non-vendor coordinators in MPCVD settings where there is no clear owner of the technology leading the coordination (mitigating vendor). A non-vendor coordinator can assist in MPCVD by:

— Coordinating the triage and mitigation across multiple vendors both within and across a specific industry sector.

— Facilitating the exchange of information between reporters of a security vulnerability and those affected by it.

— Establishing an NDA and/or system for compartmentalizing the exchange of confidential information between independent entities (e.g. reporters, vendors, industry groups) during the embargo period.

6.4 Reporters

ISO/IEC 29147 provides the description and definition of a reporter. Often this is a single entity reporting a vulnerability to a vendor. In cases of MPCVD, there can be multiple reporters of the same vulnerability that surface at the start of, or during an embargo. These additional reporters add a more complex dynamic to the coordination of the triage, mitigation, disclosure and exchanges of information for the specific vulnerability.

6.5 Users

Users or end-users can take necessary action once a remediation is available. More information about users can be found in ISO/IEC 29147:2018, 5.5.2.

6.6 Product security incident response team (PSIRT) function

ISO/IEC 30111 provides the description and definition of staff capabilities for PSIRTs. Organizations can prepare for MPCVD by implementing the foundational processes found in ISO 29147 and ISO/IEC 30111. In cases of MPCVD, the PSIRT is the primary coordinator of triage, mitigation, disclosure and any information exchanges inside and outside the vendor.

7 MPCVD life cycle

7.1 General

Clause 7 describes the life cycle of MPCVD and expanding on elements found in ISO/IEC 29147 and ISO/IEC 30111.

7.2 Policy development

7.2.1 Preparation

A vendor prepares for MPCVD by establishing foundational processes found in ISO/IEC 29147 and ISO/IEC 30111. Additional considerations to support MPCVD are below.

7.2.2 Policy

In addition to the recommended policy elements found in ISO/IEC 29147, a vendor considers:

— Including expectations for MPCVD within their external vulnerability disclosure policy and bug bounty if applicable. This can include considerations related to legal terminology facilitating explicit authorization for reporters and clarification related to potential legal consequences of reporting ("safe harbour") and third-party rights [see ISO/IEC 29147:2018, 9.4.2 (for more information see, e.g. Disclose.io)].

— Displaying appropriate contact information for their vulnerability disclosure program on their public corporate website to help ensure open lines of communication with vulnerability reporters, vulnerability coordinators, other vendors and members of their supply chains.

— Establishing a program to help ensure open lines of communication for and maturing relationships with vulnerability reporters to address the specific complexities and considerations associated with MPCVD.

— Establishing and maintaining relationships with anticipated dependent vendors in the supply chain to prepare for the handling of a vulnerability that requires MPCVD and supportive processes.

— Partnering and collaborating with other vendors affected by the same vulnerability that can aid in the vulnerability mitigation development and disclosure coordination.

7.3 Strategy development

7.3.1 Information sharing strategy

An information sharing strategy between stakeholders (e.g. vendors, internal teams, reporters and customers) can be developed prior to engaging in MPCVD to assist the process. Ideally, the strategy is designed to be flexible since the complexity of vulnerabilities and the list of stakeholders can vary from case to case. The mitigating vendor considers the strategy concerning sharing information about a vulnerability, with impacted downstream stakeholders during mitigation development, for the purpose of minimizing exposure[2]. In this document, considerations for disclosure have been outlined in Clause 11. Additionally, regular updates are typically provided to the vulnerability reporter as needed.

7.3.2 Disclosure strategy

The considerations related to the disclosure strategy are outlined hereafter. The mitigating vendor or coordinator (when applicable, in the case of the non-owner MPCVD case) typically determines the embargo period and public disclosure date, based on these considerations. As explained in the scope, MPCVD can considerably increase the disclosure timeline/embargo period due to the increased collaboration of different vendors often needed, as well as the subsequent necessary actions, which can be subject to varying engineering schedules. The vehicle or methodology for disclosure can also vary based on the needs of the MPCVD participating vendors.

A non-vendor coordinating organization can be used to support and aid the MPCVD, as appropriate, in case there is no mitigating vendor leading the coordination efforts (see 6.3).

7.4 Know your customers

Due to the complexity of MPCVD, vendors generally understand the needs of their customers with respect to incorporating security vulnerability mitigations into their respective product portfolios. As described in 9.6, there are instances where downstream vendors or dependencies are unknown, among others given the supply chain of downstream vendors is complex or lacks transparency. The mitigating vendor typically provides reasonable and timely communication (depending on the circumstances and considerations of the MPCVD process) to their stakeholders so the vulnerability mitigation can be incorporated, tested and deployed in the affected downstream vendor's affected products prior to public disclosure.

7.5 Encrypted communication methods and conference calls

Encrypted communications are integral for securing vulnerability information with multiple parties. See ISO/IEC 29147:2018, 5.8.2 for more information on secure communications.

Vendors set expectations for communication and ensure all parties involved in MPCVD are using the agreed communication method. This can include the primary vendor or a coordinating organization, hosting regular conference calls during the embargo period to help stakeholders remain aligned on the agreed mitigation and disclosure strategies.

7.6 Processes and controls

In addition to applying the process and controls outlined in ISO/IEC 29147 and ISO/IEC 30111 in order to handle a reported vulnerability, the following areas can be integrated into the process for MPCVD.

In cases where MPCVD is employed, there will be a need to exchange confidential information between a range of stakeholders both within and outside of the coordinating vendor or organization. In these cases, additional diligence is needed to help ensure the data exchanged, communication methods and, in some cases, the identities of those involved remain confidential as part of the agreed disclosure strategy. Vulnerability process additions can include:

— Evaluating and choosing an encrypted persistent chat application.

— A system of watermarking or tagging confidential information exchanged with all stakeholders during the embargo period.

— An agreement with reporters that outlines how and when their information is provided to stakeholders and/or other reporters that can have encountered a similar vulnerability.

— Establishing a non-disclosure agreement (NDA) that is signed by stakeholders to help ensure clarity of the terms of the embargo and requirements of confidentiality between vendor stakeholders.

8 MPCVD life cycle for each product

8.1 Product and user mapping

Given the complexity of product supply chains, downstream vendors who use code created by the vendor coordinator are considered during MPCVD. An up-to-date list allows for a vendor to determine a notification strategy during MPCVD at the release stage (public disclosure). This list is updated during the post-release phase outlined in ISO/IEC 30111.

8.2 Component analysis

Upstream vendors, or those who create code for other vendors to incorporate into products, are considered during MPCVD. A proper mapping can be accomplished by listing and maintaining the components used in vendors' product portfolio. Once a vendor creates a component list, the vendor

conducts a detailed analysis to understand the provenance of the code. In the event the code is maintained by an upstream vendor, then it is documented appropriately.

8.3 User analysis

End users, or those who take advantage of the technology and interact with the products, are also considered during MPCVD. An understanding of end-user needs is critical when developing a communications strategy during the release stage (public disclosure). End users apply mitigations once those are available.

9 MPCVD life cycle for each vulnerability

9.1 Receipt

Consistent with ISO/IEC 30111, MPCVD begins when a vulnerability report is received by a vendor. Vulnerability reports can be shared by other vendors, vulnerability reporters or third-party coordinators.

Receipt of the vulnerability report is crucial as it allows for the reporter to determine scope, and eventually for the appropriate parties to share vulnerability details and eventual mitigation information. See ISO/IEC 30111 for additional details regarding receipt.

9.2 Verification

In addition to verification elements found in ISO/IEC 30111, vendors consider the following during MPCVD:

— If a party determines the root cause of a vulnerability is in another vendor product, the vulnerability is communicated to that vendor either directly or through a non-vendor coordinator, or existing established practices for vulnerability reporting. Dependent vendors are typically added to any information sharing efforts to help ensure effective mitigation and disclosure of the vulnerability, as needed. This vendor (owner of the underlining vulnerable technology) typically assumes leadership of the coordination of this MPCVD as the mitigating vendor (see 6.2.1) best-positioned to develop the mitigation.

— If mitigating vendors determine further investigation into impacted versions is needed, the results of that investigation are typically shared with dependent vendors. The dependent vendors then assess whether they have additional impacted products based on the results of the mitigating vendor.

— MPCVD can be a factor when determining urgency of some phases of the vulnerability handling process such as vulnerability verification. If possible, reporters are encouraged to report the vulnerability directly to the mitigating vendor, the clear owner of the vulnerable technology development/identified root cause, who is typically best-situated to lead the coordination effort, accelerate the process and avoid unnecessary delay.

— Since MPCVD collaboration is typically needed in the vulnerability verification stage, in some MPCVD cases, this phase can take a longer period of time.

— Recognizing the complexity of CVD processes, including in MPCVD settings, ISO/IEC 29147 and ISO/IEC 30111 do not recommend particular timelines but rather propose that the mitigating vendor leading the coordination effort balance the goal of developing the remediation as soon as possible "with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues", as well as the need to ensure the completeness and effectiveness of the proposed mitigation, including the involvement of the relevant parties.

— MPCVD can require subsequent updates to the reporter depending on how many vendors and products are impacted.

9.3 Remediation development

In addition to remediation development efforts found in ISO/IEC 30111, there can be cases where proper remediation of a vulnerability requires the group of vendors to collaborate on remediation development in a phased approach.

MPCVD process can increase the urgency of the remediation verification process. Ideally, mitigating and dependent vendors, reporters and non-vendor coordinators are in lockstep throughout the vulnerability response process. MPCVD can increase the priority for mitigating vendors to develop remediations and subsequently, increase the priority for dependent vendors to test and integrate the proposed remediation into the dependent vendor's products, and report relevant findings to the mitigating vendor.

Dependent vendors work collaboratively to test the proposed remediations from mitigating vendors in various environments for their respective products prior to public disclosure, and report findings (see Figure 1) to inform the remediation development. Remediations are released simultaneously at the public release stage.

9.4 Release

See ISO/IEC 30111 for release information.

9.5 Post-release

See ISO/IEC 30111 for post-release information.

9.6 Embargo period

One of the key objectives of vulnerability disclosure and handling is to reduce users' risk and potential cost associated with the vulnerability. In the MPCVD case, this includes ensuring mitigating and dependent vendors can integrate the remediation and verify the proposed mitigation in various environments prior to public disclosure.

MPCVD inherently involves more vendors and other stakeholders than a typical CVD process. This increased complexity amplifies stakeholder concerns for the completeness and effectiveness of proposed mitigations (including coordinated release which can lead to increased end-user adoption).

Specifically, in the context of the handling process and embargo period timelines, ISO/IEC 29147 and ISO/IEC 30111 recognize the complexity of CVD processes, that can differ according to the technological environment, including in MPCVD settings. As a result of the increased complexity inherent to the coordination across multiple parties, many assumptions regarding the appropriate duration of CVD embargo periods do not apply. ISO/IEC 29147 and ISO/IEC 30111 do not recommend particular timelines, but rather propose that the mitigating vendor leading the coordination effort to balance the goal of developing the remediation as soon as possible "with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues", as well as the need to ensure the completeness and effectiveness of the proposed mitigation.

Organizations involved in MPCVD efforts can consider the appropriateness of any embargo period based on this balance, while considering a variety of factors, including:

— the time needed to identify and notify affected vendors and stakeholders;

— the number and diversity of relevant stakeholders identified;

— those stakeholders' degree of familiarity and willingness to cooperate with the MPCVD process;

— the time needed by MPCVD participants (i.e. dependent vendors) to develop, test and possibly deploy mitigations;

— the risk of actions by MPCVD participants resulting in early disclosure balanced with the need to maintain information in confidence.

Organizations playing a coordination role in MPCVD typically seek to strike a balance between the need for time to develop and test fixes and the risk of an embargo failure, whether by a participant's accidental or intentional acts, or independent discovery by other parties, including adversaries.

When the degree of trust among affected stakeholders is high, organizations can choose a longer embargo duration to accommodate coordination of mitigation development and testing across complex supply chains.

Organizations work to establish and maintain a high degree of mutual trust among likely MPCVD participants outside of the process of handling individual cases.

When the degree of trust among affected stakeholders is low, organizations can choose to shorten or accelerate typical embargo durations, subject to the considerations listed above.

Examples of low trust situations include:

— a large number of vendors are affected, some of whom are new to the MPCVD process;

— the supply chain for delivering mitigations to downstream vendors is complex or lacks transparency;

— affected vendors have not previously demonstrated their willingness and ability to maintain long embargo periods;

— affected vendors' disclosure policies are incompatible with extended embargo periods;

— the number of affected vendors remaining unnoticed by the coordinating parties is likely a sizable fraction of the known affected vendors;

— evidence and/or indications of threat actor awareness or use of the vulnerability are already known.

MPCVD coordinators can choose to implement a phased-participation approach toward ecosystem vendors that are essential to the remediation development effort (e.g. in remediation development, i.e. beta release or validation stage).

MPCVD stakeholders can choose to avoid entering into an embargo period or to exit an existing one, for a vulnerability when there is evidence of exploitation of that vulnerability by adversaries.

MPCVD stakeholders can choose to avoid entering into an embargo period or to exit an existing one, if the effects of a vulnerability's exploitation against their users or constituency are disproportionately worse than the effects against other affected stakeholders' users or constituency.

10 Information exchange

ISO/IEC 29147:2018, 5.7 provides a simplistic example of information exchange during vulnerability handling and disclosure. In cases of MPCVD, information exchanges are more frequent to ensure multiple vendors, reporters and/or third-party coordinators are in lockstep. Any information exchanged needs to be encrypted and secured.

The primary information exchanges for MPCVD are:

— One or more reporters sends a potential vulnerability report to one or more vendors.

— The notified vendors share receipt of the vulnerability to the reporter.

— The notified vendors can share the verification of a vulnerability report with the impacted group and/or the vulnerability reporter.

— The originating impacted vendor (mitigating vendor) shares mitigation information to dependent vendors. Issues surrounding the mitigation can be shared among the impacted vendors.