INTERNATIONAL STANDARD

ISO/IEC 29147

Second edition
2018-10

Information technology — Security techniques — Vulnerability disclosure

Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité

Reference number
ISO/IEC 29147:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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 http://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.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29147:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

— a number of normative provisions have been added (summarized in Annex D);

— numerous organizational and editorial changes have been made for clarity.

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.

This document is intended to be used with ISO/IEC 30111.

Introduction

In the contexts of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.

Vulnerabilities often result from failures of a program or system to securely handle untrusted or unexpected input. Causes that lead to vulnerabilities include errors in coding or configuration, oversights in design choices, and insecure protocol and format specifications.

Despite significant efforts to improve software security, modern software and systems are so complex that it is impractical to produce them without vulnerabilities. Risk factors of vulnerabilities include:

— operating and relying on systems that have known vulnerabilities;

— not having sufficient information about vulnerabilities;

— not knowing that vulnerabilities exist.

This document describes vulnerability disclosure: techniques and policies for vendors to receive vulnerability reports and publish remediation information. Vulnerability disclosure enables both the remediation of vulnerabilities and better-informed risk decisions. Vulnerability disclosure is a critical element of the support, maintenance, and operation of any product or service that is exposed to active threats. This includes practically any product or service that uses open networks such as the Internet. A vulnerability disclosure capability is an essential part of the development, acquisition, operation, and support of all products and services. Operating without vulnerability disclosure capability puts users at increased risk.

The term “vulnerability disclosure” is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information. Additional activities such as investigating and prioritizing reports, developing, testing, and deploying remediations, and improving secure development are called “vulnerability handling” and are described in ISO/IEC 30111. The term “disclosure” is also used more narrowly to mean the act of informing a party about a vulnerability for the first time (see 3.2).

Major goals of vulnerability disclosure include:

— reducing risk by remediating vulnerabilities and informing users;

— minimizing harm and cost associated with the disclosure;

— providing users with sufficient information to evaluate risk due to vulnerabilities;

— setting expectations to facilitate cooperative interaction and coordination among stakeholders.

The processes described in this document aim to minimize risk, cost, and harm to all stakeholders. Due to the volume of reported vulnerabilities, lack of accurate and complete information, and other factors involved, it is not possible to create a single, fixed process that applies to every disclosure event.

The normative elements in this document provide minimum requirements to create a functional vulnerability disclosure capability. Vendors should adapt the additional informative guidance in this document to fit their particular needs and those of users and other stakeholders.

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

— guidelines on receiving reports about potential vulnerabilities;

— guidelines on disclosing vulnerability remediation information;

— terms and definitions that are specific to vulnerability disclosure;

— an overview of vulnerability disclosure concepts;

— techniques and policy considerations for vulnerability disclosure;

— examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 30111, *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 27000 and the following apply.

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

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

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

3.1
vulnerability
functional behaviour of a product or service that violates an implicit or explicit security policy

Note 1 to entry: ISO/IEC 27002:2013, 12.6.1[1] uses the term "technical vulnerability" to distinguish between the more general risk-based concept of vulnerability and the term used in this document.

3.2
disclosure
act of initially providing *vulnerability* (3.1) information to a party that was not believed to be previously aware

3.3
coordination
set of activities including identifying and engaging stakeholders, mediating, communicating, and other planning in support of *vulnerability* (3.1) *disclosure* (3.2)

Note 1 to entry: The term "coordinated vulnerability disclosure" is used to denote a disclosure process that includes coordination.

3.4
vendor
individual or organization that is responsible for remediating vulnerabilities

Note 1 to entry: A vendor can be the developer, maintainer, producer, manufacturer, supplier, installer, or provider of a product or service.

3.5
reporter
individual or organization that notifies a *vendor* (3.4) or *coordinator* (3.6) of a potential *vulnerability* (3.1)

Note 1 to entry: There are no special requirements for acting as a reporter. Reporters can be individuals, organizations, amateurs or hobbyists, professionals, end-users, security research organizations, vendors, governments, or coordinators.

Note 2 to entry: The term "reporter" does not imply unique or original discovery or reporting.

Note 3 to entry: Reporters can be called researchers, whether or not the reporter explicitly performs security or vulnerability research. Historically, this role is also referred to as "finder."

3.6
coordinator
individual or organization that performs *coordination* (3.3)

3.7
remediation
change made to a product or service to remove or mitigate a *vulnerability* (3.1)

Note 1 to entry: A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for "remediation" include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

3.8
advisory
document or message that provides *vulnerability* (3.1) information intended to reduce risk

Note 1 to entry: An advisory is meant to inform users or other stakeholders about a vulnerability including, if possible, how to identify and remediate vulnerable systems.

4 Abbreviated terms

COTS	common off-the-shelf
CRM	customer relationship management
CSIRT	computer security incident response team
CVE	common vulnerabilities and exposures[9]
CVRF	common vulnerability reporting format[12][13]
CVSS	common vulnerability scoring system[10]
CWE	common weakness enumeration[11]
HTTP(S)	hypertext transfer protocol (secure)
ICT	information and communication technology
OpenPGP	open pretty good privacy
OWASP	open web application security project
PoC	proof of concept
PSIRT	product security incident response team
S/MIME	secure multipurpose internet mail extensions
SQL	structured query language
TLS	transport layer security

5 Concepts

5.1 General

The purpose of this clause is to provide background information and context to help understand vulnerability disclosure.

Vulnerability disclosure involves different stakeholders with different perspectives, incentives, capabilities, and available information. Furthermore, communication and process synchronization among multiple stakeholders can quickly become complicated. In practice, disclosure can deviate from the activities described in this document due to a variety of unforeseen circumstances.

5.2 Structure of this document

This document is meant to be read in its entirety as input to the development or improvement of vulnerability disclosure policies and processes. The remaining clauses of this document are organized as follows:

— Clause 5: Concepts;

— Clause 6: Receiving vulnerability reports;

— Clause 7: Publishing vulnerability advisories;

— Clause 8: Coordination;

— Clause 9: Vulnerability disclosure policy.

The structure of this document is not meant to be followed in strict sequence as it appears above. For example, a vendor should ideally develop policy (Clause 9) before starting to receive reports (Clause 6).

Annex D contains a summary of all of the normative elements in this document.

5.3 Relationships to other International Standards

5.3.1 ISO/IEC 30111

ISO/IEC 30111 shall be used in conjunction with this document. The relationship between the two International Standards is illustrated in Figure 1.

This document 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.

ISO/IEC 30111 gives guidelines on how to investigate, process, and resolve potential vulnerability reports.

While this document deals with the interface between vendors and 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.

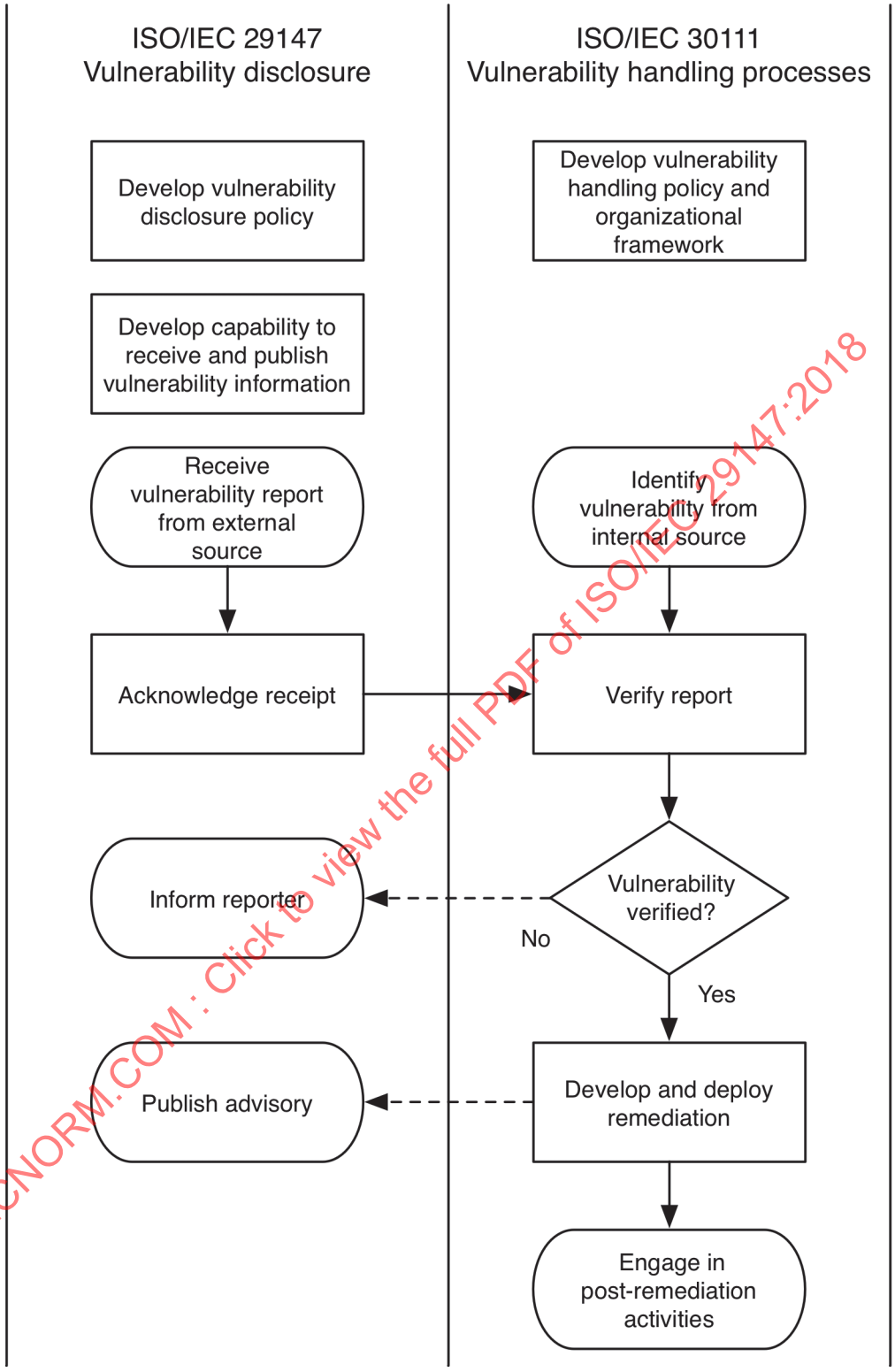

Figure 1 — Relationship between ISO/IEC 29147 and ISO/IEC 30111

5.3.2 ISO/IEC 27002

Vulnerability disclosure enables the management of technical vulnerabilities (ISO/IEC 27002:2013, 12.6.1[1]).

5.3.3 ISO/IEC 27034 series

Application security seeks to reduce the creation of application vulnerabilities (see ISO/IEC 27034-1:2011, 6.5.2[4]). Vulnerability disclosure can demonstrate the need for changes to application security practices. Vulnerability disclosure cannot demonstrate that application security is completely effective.

Vulnerability disclosure occurs in the utilization and maintenance phases of the application security lifecycle reference model described in ISO/IEC TS 27034-5-1:2018, 6.3.13 and 6.3.14[5].

5.3.4 ISO/IEC 27036-3

Vulnerability disclosure supports multiple aspects of ICT supply chain security described in ISO/IEC 27036-3:2013, 5.4 a), 5.8 i), 6.1.1 a) 2) and 6.3.4 [7].

5.3.5 ISO/IEC 27017

Vulnerability disclosure is necessary to enable the management of technical vulnerabilities as specified for cloud services in ISO/IEC 27017:2015, 12.6.1[3].

5.3.6 ISO/IEC 27035 series

Some incident management plans, particularly those of vendors, include vulnerability disclosure (see ISO/IEC 27035-1:2016, Introduction[6]). Such plans typically treat vulnerability disclosure as a type of incident. Incident management can also include vulnerability management (see also ISO/IEC 27002:2013, 12.6.1[1]), which is only possible when vulnerabilities are disclosed.

5.3.7 Security evaluation, testing and specification

This document provides guidance for vulnerability reports received externally, and not through organized internal assurance and evaluation efforts. Thus, the more formal testing, assurance, and evaluation standards ISO/IEC 15408[15] and ISO/IEC 18405[16] do not generally apply.

5.4 Systems, components, and services

5.4.1 Systems

A system is a set of connected components and services. In vulnerability disclosure, the causes of a vulnerability can be unclear, or due to interactions between the parts of a system, or between systems. Thus, it is sometimes necessary to talk about systems being affected by vulnerabilities.

5.4.2 Components

A component is a unit of software or hardware that can be both an entire system unto itself and used as part of a larger system. A component can be an entire operating system, a chip, an application, a package, a library, or even a single file or segment of source code.

For the purposes of this document, the distinction between hardware and software components is seldom relevant. There are very few cases of vulnerabilities in pure hardware components. In most cases, so-called “hardware” vulnerabilities actually occur in low-level software or firmware.

5.4.3 Products

A product is usually one or more components or a system. Products are provided by vendors to users either for sale or for free, usually under licensing terms. There are many different types of products including but not limited to, custom software built under contract for a specific user’s licenced use, libraries intended to be included in other products, commercial off-the-shelf (COTS) products for mass markets, community-developed projects, and recreational or hobbyist offerings.

5.4.4 Services

A service is a collection of features provided to users. Users can interact with services they do not own, operate, or maintain.

For vulnerability disclosure, vulnerabilities in services maintained by the vendor can usually be remediated by the vendor taking action. Users can have to take action as well in order to remediate the vulnerability. For example, a vendor implements changes on their own infrastructure to remediate the vulnerability, and users have to change their passwords after the vendor has implemented the changes.

5.4.5 Vulnerability

A vulnerability is generally a behaviour or set of conditions that allows the violation of an explicit or implicit security policy. Typically, the violation of a user's security policy results in a negative impact or loss to the user. One common way to categorize loss is to consider the impact to the confidentiality, integrity, and availability of an asset. For example, a vulnerability that allowed an attacker to install malicious software on a user's system impacts confidentiality and integrity since the attacker can use the malicious software to read or change sensitive information. A vulnerability in a network product that caused the product to experience a system error would impact availability. The actual impact of a vulnerability depends on how the vulnerable product is used and other contextual factors.

Vulnerabilities are often caused by implementation defects in software. A vulnerability can be associated to the security policy if one exists. One common type of vulnerability includes buffer overflows and related low-level memory management errors that allow specially crafted input to control execution of the vulnerable software program. SQL injection and cross-site scripting vulnerabilities are common types of vulnerabilities found in web applications. Many other sets of conditions can cause or contribute to vulnerabilities, including design decisions, default configuration settings, weak authentication or access control, lack of awareness or education, or even unexpected interactions between systems or changes in operating environments.

More information about types of vulnerabilities can be found in CWE and OWASP. Both of these resources help developers and engineers to recognize and avoid creating security vulnerabilities.

Many stakeholders (predominantly vendors and users) seek to identify and resolve vulnerabilities, either removing them entirely (usually by patching or updating software to remove defects) or by mitigating or working around vulnerabilities to reduce the likelihood or impact of successful attack. Vulnerability disclosure provides vendors and users with information to resolve and mitigate vulnerabilities and to make better risk decisions.

Attackers also seek to identify vulnerabilities, but typically do not attempt to disclose or resolve vulnerabilities. Attackers seek to exploit vulnerabilities for some gain, almost always causing loss to users.

5.4.6 Product interdependency

Many products are complex systems that include or are dependent upon other products or components in some way. It is possible that a user or vendor is not initially be certain which products are affected by the vulnerability. These interdependencies are important since products that use or interact with a vulnerable product can also be vulnerable.

product dependencies can include:

— source code re-use from other products, software libraries, or other types of interfaces;

— hardware or software supply chain;

— rebranding by different vendors of the same core technology;

— use of the same protocols or formats.

Depending on sales, distribution, and support models, vendors can have accurate lists of users or not. This can be relevant when considering notifying affected users of a vulnerability.

5.5 Stakeholder roles

5.5.1 General

This subclause describes significant stakeholder roles in vulnerability disclosure. Stakeholders are individuals, groups, or organizations that act in one or more roles.

5.5.2 User

Users can directly operate software or hardware products or make use of a service. Users can be referred to as consumers, customers, or end-users. Due to the interdependencies of modern software products, users might not know precisely which products or services they are actually using.

Users need information about vulnerabilities, particularly remediation, in order to make effective risk decisions and to use software products and services more securely. Publishing vulnerability information is discussed in Clause 7.

5.5.3 Vendor

There are a number of different terms used to describe individuals or organizations who create or provide software products, including manufacturer, developer, maintainer, or distributor. Similarly, an individual or organization that delivers software products within a supply chain can be called a supplier. For the purposes of this document, the term "vendor" is used to mean all of these individuals and organizations. A vendor can be an individual, a small team, a large commercial enterprise, or an open source project.

Vendors are responsible for the security of their products and services. Vendors carry out vulnerability disclosure to receive reports about vulnerabilities, develop remediations, and publish advisories.

There are many types of vendors with various models for developing, selling, supporting, and distributing products. Some vendors integrate products into a system or service, and these vendors may act as customers or users of the component products. Such vendors can be dependent on component vendors for vulnerability remediation information.

5.5.4 Reporter

The reporter notifies a vendor of a potential vulnerability. A reporter usually, but not always, finds or discovers the vulnerability. The discovery may not be the first or only discovery. For the purposes of this document, it is assumed that a reporter will attempt to inform a vendor or coordinator about a vulnerability. In practice, a reporter can choose not to attempt to inform a vendor or coordinator, or the attempt can fail. Receiving vulnerability reports is discussed in Clause 6.

A reporter is often a security researcher, but it is important to reinforce that any individual or organization can act as a reporter. Professional researchers can operate independently or as part of an organization. Some researchers are associated with universities or other academic institutions. Other reporters do not regularly perform security analysis or research but identify vulnerabilities in the course of other activity or even by accident. Vendors, users, and coordinators can all act as reporters.

The variety of reporters has implications for the quality of vulnerability reports and the familiarity of the reporter with disclosure practices.

Reporters are sometimes concerned with legal or other pressure brought to bear on them. Such pressure can have a "chilling effect," decreasing the likelihood of reporting.

5.5.5 Coordinator

A coordinator generally acts as intermediaries between a reporter and vendor. Common services provided by a coordinator include:

— identifying and contacting vendors;

— managing vulnerabilities that affect multiple vendors;

— performing technical analysis and validation;

— negotiating disclosure timelines;

— supporting reporters;

— publishing advisories;

— educating vendors and reporters about the disclosure process.

It is not necessary for coordinators to be involved in every disclosure. For cases involving one or a small number of vulnerabilities affecting a single vendor, a reporter and vendor are often sufficient. Coordinators can aid negotiations when multiple vendors are affected, reporters and vendors disagree, or other complexities arise.

Coordinators may work with other coordinators to obtain help with domain expertise, language, geographic, and cultural barriers and to share resources and effort. Some computer security incident response teams (CSIRTs) provide broad vulnerability coordination services on an operational basis, while other CSIRTs coordinate in more limited ways, for example, covering specific regions, industries, or on an as-needed basis.

Some vendors and governments provide free coordination services while some vendors offer commercial coordination services.

Some vendors provide coordination services, as do some commercial security vendors. For example, some organizations pay reporters for vulnerability reports, use the vulnerability information to provide commercial protection to their customers, and also act as coordinators, disclosing privately to vendors and later to the public. There are variations and degrees of commercially-oriented vulnerability coordination offerings.

While coordinators often have interests in protecting their constituencies, coordinators should attempt to be technically objective and minimize risk to all stakeholders.

Coordination is further described in Clause 8.

5.6 Vulnerability handling process summary

5.6.1 General

This subclause summarizes the vulnerability handling process that is described further in ISO/IEC 30111. Figure 2 outlines the vendor's vulnerability handling process including a preliminary step to develop a vulnerability disclosure policy and capabilities.

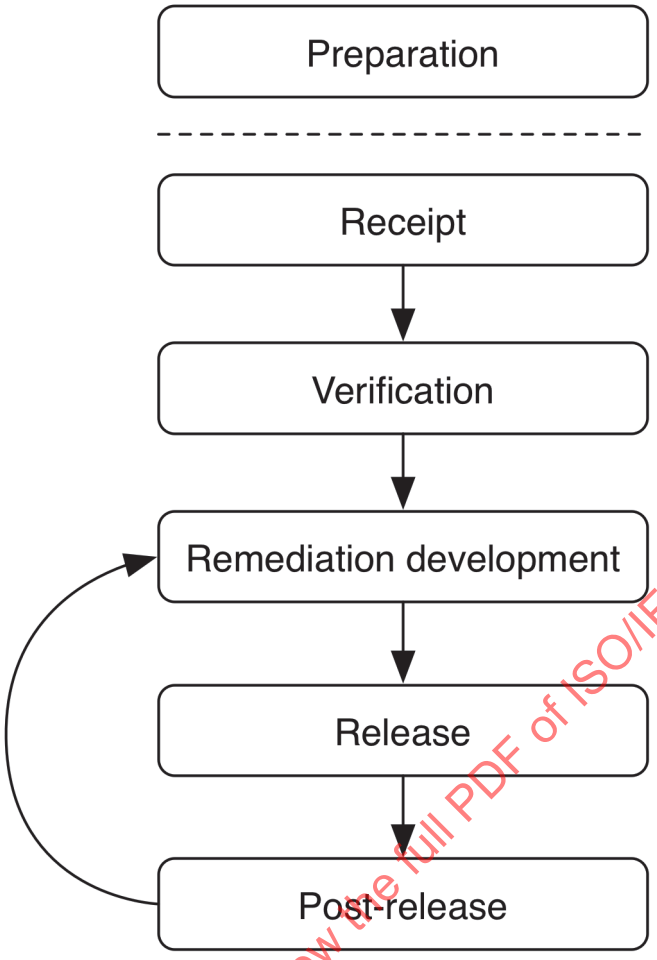

Figure 2 — Summary vulnerability handling process

5.6.2 Preparation

Vendors should develop policy (see Clause 9), processes, and capability before starting a vulnerability disclosure program. Preparation can involve creating a response organization (often called a PSIRT or CSIRT), hiring and assigning staff, developing tools, and publishing information about the program.

Vendors should consider performing vulnerability assessments of products and services in scope of the program. Such assessments can identify easily discovered vulnerabilities and reduce the number of reports before the program starts.

5.6.3 Receipt

A reporter identifies potential vulnerabilities in products or services and notifies the vendor. The vendor acknowledges receipt of the report.

If a vendor is not able to receive a vulnerability report, the reporter or coordinator may decide to publish an advisory without the vendor's prior knowledge. A reporter, or anyone in possession of vulnerability information can disclose or publish the information at any time.

Receiving vulnerability reports is described in Clause 6.

5.6.4 Verification

The vendor investigates the report. Investigation often involves attempting to reproduce the environment and behaviour reported by the reporter. This can be a preliminary investigation, focused primarily on the need for further effort by the vendor. Investigation can also include correlating similar or related reports, assessing severity, and determining other affected products. The investigation determines whether the report constitutes a vulnerability or not. The vendor may communicate with the reporter during the investigation, and the vendor notifies the reporter of the results at the end of the investigation. This phase is often called “triage.”

5.6.5 Remediation development

The vendor develops remediations for vulnerabilities. Remediation development can involve more detailed investigation of the root cause of the vulnerabilities and determination of other products affected by the same or similar vulnerabilities. The vendor typically develops remediation and mitigation techniques and performs positive tests to determine that the remediation works correctly, and negative (regression) tests to provide assurance that the remediation does not disrupt existing functionality.

The vendor should feed the information about the vulnerability and root cause analysis back into the software development lifecycle or deployment guidelines, in order to avoid introducing the same type of vulnerability in the future. See also ISO/IEC 27034-1[4].

5.6.6 Release

The vendor develops and securely distributes the remediation. For a product, the vendor provides the remediation and mitigation information to users, typically in the form of a vulnerability advisory and software patches or updates, and users deploy the remediation.

For a service vulnerability, the vendor deploys remediation and optionally discloses the vulnerability.

A vendor may release an advisory before a remediation is available, particularly in cases of active exploitation or public discussion. The vendor should attempt to ensure the remediation does not introduce new vulnerabilities, overall product quality issues, or have compatibility problems with other products or services if possible.

An important reason for informing users about a vulnerability is that users often need to take action to remediate and re-assess their risk. When remediating a vulnerability in a service, it is possible that there is no need for users to take any action. There are, however, other reasons to publish vulnerability information, including:

— support for incident or forensic investigations, knowing when a vulnerability existed (and was not remediated);

— improved secure design, engineering, and development practices;

— transparency and accountability, informing users and other stakeholders that vulnerabilities are identified and remediated;

— assurance, informing users of non-vulnerability;

— providing authoritative information, disambiguation, clarification;

— informing public policy decisions;

— documenting system changes for development and operational use;

— providing acknowledgment and credit to reporters.

Considering reasons beyond the need for user action, a service can still choose to publish vulnerability information.

Publishing vulnerability advisories is described in Clause 7.

5.6.7 Post-release

A vendor collects feedback from users and updates remediation and mitigation information as necessary. For example, a remediation can be found to be incomplete or to cause regression issues or side effects.

5.6.8 Embargo period

In order to give vendors time to develop remediations without attackers also having access to public vulnerability information, reporters often notify vendors privately and do not disclose publicly until remedations are ready or an embargo period has elapsed. The receipt, verification, and remediation development phases are typically covered by the embargo period. Reporters and other with knowledge of a vulnerability have the ability to disclose publicly at any time. Reporters use different embargo periods, which are sometimes negotiable.

5.7 Information exchange during vulnerability disclosure

Figure 3 illustrates information exchange during vulnerability disclosure. There are two main exchanges: Potential vulnerability reports from reporters to vendors, and advisories from vendors to users. A potential vulnerability report is sent from a reporter to a vendor either directly or through a coordinator. A vendor may act as a reporter and report a vulnerability to another vendor. An advisory is released by a vendor either privately to its users or, more commonly, to the public. This document focuses on these two exchanges from the perspective of the vendor receiving vulnerability reports and publishing remediation information.

A complete vulnerability disclosure process can include multiple disclosure events, such as a reporter reporting to a vendor, a vendor publishing an advisory, or a coordinator notifying other vendors.

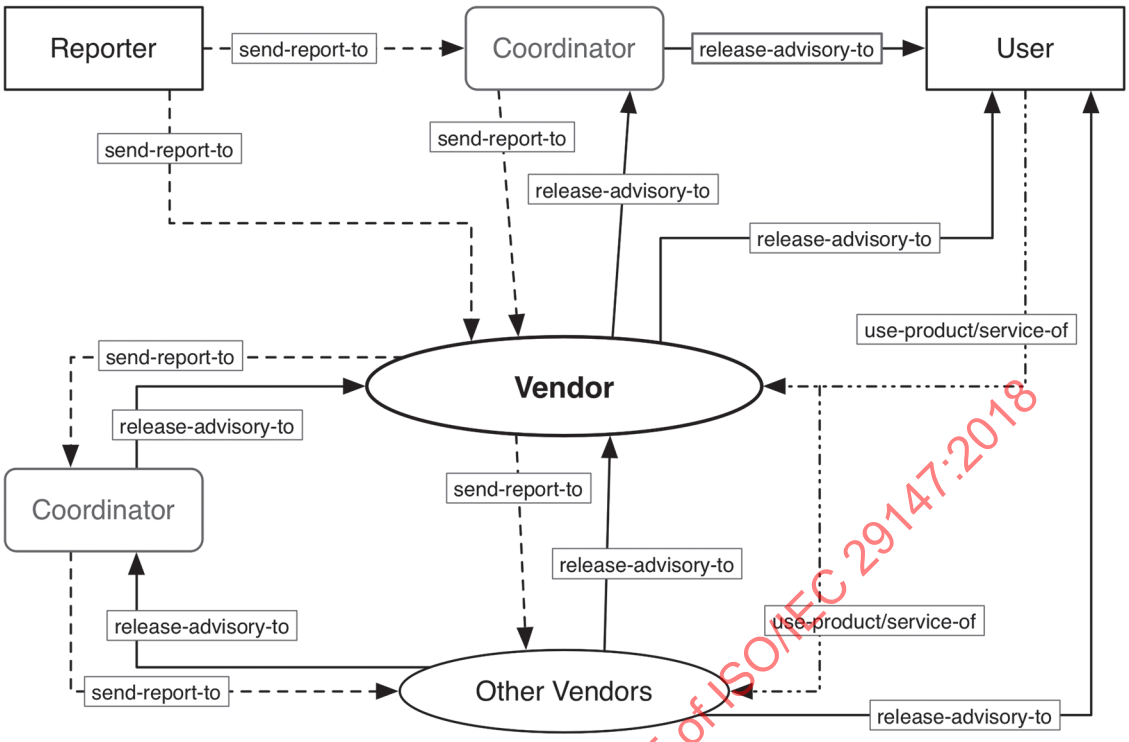

Figure 3 — Vulnerability information exchange

5.8 Confidentiality of exchanged information

5.8.1 General

Since vulnerability information can be used to attack vulnerable systems, sensitive vulnerability information should be communicated confidentially, particularly when the information is not publicly available.

5.8.2 Secure communications

Vendors should provide secure confidential methods for reporters to report vulnerability information. Message integrity is also important, particularly in verifying that remediation information is authentic. Common cryptographic protocols and implementations such as TLS, S/MIME, and OpenPGP can provide confidentiality and integrity. If there are other security requirements, ISO/IEC 27010[2] can be relevant. An example would be if a coordinator offers a reporter anonymity service.

5.9 Vulnerability advisories

Vulnerability information is generally published in an advisory. The advisory describes the vulnerability, usually focusing on remediation and mitigation, but can also include information about affected systems, threats, impact, and references. Users reading an advisory need sufficient information to make informed risk decisions about how to remediate or mitigate the vulnerability.

Publishing vulnerability advisories is described in Clause 7.

5.10 Vulnerability exploitation

In general, attackers seek to exploit vulnerabilities for some gain, almost always causing loss to users. Various factors such as target population, exposure of targets, value of targets to the attacker, and cost of exploit development, can influence whether or not a vulnerability will be exploited by attackers. Any attempt, however, to predict whether or not a vulnerability will or has already been used in attacks can be subject to considerable uncertainty. The most conservative assumption is that a vulnerability can and will (and can have already been) used in attacks.

5.11 Vulnerabilities and risk

Vulnerabilities contribute to risk, particularly when exploited in attacks. Vulnerability disclosure informs stakeholders about vulnerabilities and ideally includes remediation information, leading to fixed vulnerabilities and reduced risk. Vulnerability disclosure itself creates risk, since public disclosure provides information for exploit developers and attackers. The theory supporting vulnerability disclosure holds that the short-term risk caused by public disclosure is outweighed by longer-term benefits from fixed vulnerabilities, better informed defenders, and systemic defensive improvements.

6 Receiving vulnerability reports

6.1 General

This clause provides guidance for vendors on receiving information about potential vulnerabilities. A capability to receive vulnerability reports helps vendors more quickly become aware of new reports and establish working relationships with reporters and other stakeholders.

6.2 Vulnerability reports

6.2.1 General

Reporters notify vendors of potential vulnerabilities. Reports typically include a description of what product or service is affected, how the potential vulnerability can be identified, demonstrated, or reproduced, and what type of functional impact the vulnerability allows.

Reports may include proof-of-concept (PoC) code that demonstrates exploitation of the vulnerability. Since a vulnerability report is likely to contain sensitive, non-public information, vendors should provide mechanisms to receive reports confidentially (see 5.8 and 6.7).

6.2.2 Capability to receive reports

Vendors shall provide one or more technically current and usable mechanisms to receive reports of potential vulnerabilities. This corresponds to the receipt phase described in 5.6.3.

Typical reporting mechanisms include:

— web forms;

— bug or issue tracking systems;

— vulnerability reporting services;

— e-mail, possibly an alias, list, or role address that is independent of any one individual.

Vendors should prefer secure mechanisms to receive reports, but may accept reports through less secure mechanisms such as plaintext e-mail or public bug tracking systems.

To facilitate the verification step of the vulnerability handling process, vendors should design reporting mechanisms to elicit information useful in assessing the validity, severity, scope, and impact of vulnerabilities. Such information includes:

— product or service name and affected versions;

— class or type of vulnerability, optionally using a taxonomy like CWE;

— possible root cause;

— PoC code or other substantial evidence;

— tools and steps to reproduce the vulnerable behaviour;

— impact and severity estimate;

— scope assessment, other products, components, services, or vendors thought to be affected;

— disclosure plans, specifically embargo and publication timelines.

For further examples of information to request in a report, see Annex B.

6.2.3 Monitoring

Vendors shall monitor their reporting mechanisms for new reports and communications related to existing reports. In addition, vendors should monitor public sources (including mailing lists and social media used by the security research community) for reports of vulnerabilities. Vendors should also monitor customer service and support and other organizational communications channels that are likely to receive vulnerability reports.

6.2.4 Report tracking

Vendors should use a mechanism to label (assign identifiers to) and track reports, for example, bug tracking, CRM, or ticketing systems. Vendors should provide reporters and other stakeholders with vulnerability report identifiers. Vendors may use more than one labelling and tracking mechanism, however, multiple mechanisms can cause confusion.

Other stakeholders can also use labelling and tracking mechanisms.

6.2.5 Report acknowledgement

Vendors shall acknowledge receipt of potential vulnerability reports within 7 calendar days.

The response can be automated, but should be meaningful. The response should include a tracking number or identifier, and preliminary status information. The response can indicate that the report is under investigation, or requires further information, or is considered to be incomplete, spurious, or otherwise irrelevant.

In the case of significantly inaccurate, repeated, or spurious reports, no response is necessary, or an automated response is acceptable.

The initial acknowledgement from vendor to reporter is important in establishing a working relationship. Many reporters become frustrated by the inability to report to vendors or the lack of response from vendors. Frustrated reporters are more likely to seek other means of disclosure, including public disclosure[14].

Most of the remediation development process is not visible to the reporter. It is therefore important to communicate realistic expectations and status updates to reporters.

6.3 Initial assessment

Vendors shall perform initial assessment, or triage, of vulnerability reports. This corresponds to the Verification phase described in 5.6.4. Reports can be prioritized and categorized based on severity, impact, scope, ease of exploitation, likelihood of independent discovery, and other factors.

This initial assessment phase can be tedious and time consuming. New reports should be examined carefully enough to minimize false negatives. That is, the initial assessment should be designed to have high sensitivity, correctly identifying and rejecting reports that are not vulnerabilities at the cost of accepting reports that later turn out not to be vulnerabilities. New reports should also be compared with existing reports to identify duplicates.

At this phase, vendors should take significant care to only reject reports that are strongly considered not to be vulnerabilities and do not warrant further response. In such cases, the reporter should be informed of the vendor's assessment.

If a vendor does not consider a report to be a vulnerability, the vendor shall inform the reporter and other stakeholders.

6.4 Further investigation

For reports that require further investigation or are considered to be valid vulnerabilities, vendors shall begin vulnerability handling processes. As noted in Figure 1, these processes are described in ISO/IEC 30111. Investigation and vulnerability handling correspond to the remediation development phase described in 5.6.5.

In order to perform further investigation, vendors may communicate with reporters and other internal and external stakeholders to understand the vulnerability and its impact. Vendors should request additional information from reporters as needed to fully assess or reproduce the reported vulnerability.

If other vendors are affected or likely to be affected, the initial vendor should notify the other vendors or engage a coordinator. Vendors should be aware of supply chain relationships and common usage of shared or similar components, such as libraries, protocols, and formats.

6.5 On-going communication

During vulnerability handling, vendors shall communicate with reporters and other stakeholders. Such communication should include information such as:

— status updates;

— significant new information;

— changes to existing plans;

— disclosure timing.

When there is a disagreement among stakeholders, particularly concerning public disclosure, vendors should communicate their intentions so that stakeholders are not surprised.

Supply chain relationships, or the need to involve other stakeholders during the investigation, can introduce additional delays in communications. When necessary, vendors should explain communication and process delays to stakeholders.

6.6 Coordinator involvement

Coordinators can be involved in the receiving phase. Coordinators can act as reporters, or on behalf of reporters, attempting to identify and report vulnerabilities to vendors. Coordinators can mediate between reporters and vendors. Coordinators can also provide additional support in assessing the validity, severity, impact, and scope of vulnerabilities.

Coordination is described further in Clause 8.

6.7 Operational security

Vendors should consider operational security throughout the processes of receiving and communicating about vulnerability reports.

Reporting mechanisms (see 6.2) and on-going communications (see 6.5) should provide confidentiality to limit access to sensitive, non-public vulnerability information. Reporting and communication mechanisms may also provide authentication. Reporting mechanisms should provide the ability for reporters to verify the identity of the vendor.

Typical security mechanisms include:

— web-based forms or applications using TLS (HTTPS);

— e-mail encryption and signing using S/MIME or OpenPGP.

Vendors should also consider internal operational security and limit access to non-public vulnerability information to staff and organizational units that need to know.

7 Publishing vulnerability advisories

7.1 General

This clause provides guidance on disclosing vulnerability information to users, other stakeholders, and the public. In most cases, at this phase, vendors have developed and tested a remediation for the vulnerability, having followed the processes described in ISO/IEC 30111. In most cases, vendors should publish, or publicly disclose, information about identifying and remediating the vulnerability. Publishing advisories generally corresponds to the Release phase described in 5.6.6.

7.2 Advisory

The term advisory is used broadly to mean any document or message containing vulnerability information. Advisories should be intended for widespread, usually public disclosure (publication) and should enable users to identify vulnerable products and services and take action to remediate vulnerabilities. Advisory authors should consider the needs of the intended audience and produce advisories that are effective in terms of informational content, distribution mechanisms, and presentation format.

Example advisories can be found in Annex C.

7.3 Advisory publication timing

Vendors should work to balance risk while choosing when to publish advisories. To reduce disruptions to users, vendors may publish advisories in batches and schedule releases in advance. Vendors may also publish advisories as soon as corresponding remediations are available.

If a vulnerability is being actively exploited and remediation is not available, vendors should publish advisories informing users of the current threat and what steps users can take to reduce risk until a remediation is available.

Vendors should, when possible, attempt to coordinate advisory release in instances where their products are affected by interrelated vulnerabilities. Releasing information about a vulnerability in one product can expose other interdependent products to increased risk of attack. This situation typically occurs when a software library, protocol, module or other component is used in multiple products or services, often affecting multiple vendors. It is possible that a coordinator can facilitate disclosure and advisory publication timing among multiple vendors.

Other factors to consider include:

— any embargo periods (see 5.6.8);

— expected time between publication and remediations being applied (see 5.6.6);

— reporter's agenda for publication;

— advisory release schedule of other vendors;

— possible negative side-effects of a workaround or remediation;

— language localization;

— readiness of remediation for different versions or platforms;

— readiness of customer support and sales organizations.

7.4 Advisory elements

7.4.1 General

Advisories should contain sufficient information to enable the target audience — including system administrators, developers, managers, and users — to decide if the vulnerabilities are relevant and how to remediate them.

Readers of advisories have different needs that can be dependent on market segment or regulatory requirements. Technical users such as system administrators tend to prefer detailed information about vulnerabilities and workarounds. Consumers typically appreciate information on how to determine if they are using the affected products and plain, easily understood remediation advice. Vendors should design advisories for the expected audience. A single advisory can address multiple vulnerabilities, for example, when a single remediation resolves multiple vulnerabilities.

The following subclauses describe the elements included in advisories. The list is not exhaustive and vendors may include additional elements. Unless otherwise stated, the order of the subclauses does not indicate the order of elements appearing in an advisory.

7.4.2 Identifiers

Advisories shall contain certain identifiers.

a) Advisory identifier: An advisory shall be labelled with a unique and consistent identifier for the advisory document. CVE identifiers may be used as advisory identifiers if a single advisory describes only one vulnerability. To the extent possible, CVE identifiers are assigned for individual vulnerabilities. A single advisory can address multiple vulnerabilities.

b) Vulnerability identifier: An advisory shall provide unique and consistent identifiers for vulnerabilities addressed in the advisory. Identifiers should be sufficiently unique and consistent so as to not confuse different advisories or vulnerabilities. Advisory authors should choose a common, shared vulnerability identification system such as CVE.

c) Product identifiers: An advisory should include product name and version information in order to inform readers which products are affected and optionally which products are not affected. See 7.4.6.

7.4.3 Date and time

Advisories shall indicate the date of initial publication and may include other dates, for example, as part of the revision history. Advisories shall use unambiguous date and time references and should use ISO 8601[8].

7.4.4 Title

The title of an advisory should contain a reference to a product or some other description that is informative to readers so that they can quickly decide if the advisory is relevant.

7.4.5 Overview

The overview element provides a brief, high-level summary of the vulnerability so that users can understand the salient points of the report and quickly determine if the advisory is applicable to their environment.

7.4.6 Affected products

The advisory shall provide sufficient information for users to determine if they are affected by the vulnerability or not.

This element of the advisory provides a list of known, supported, and affected products and their versions. This element may provide instructions about how to verify the version of the product. In most cases, services do not have version identifiers but can have a date when the last update or change was made.

This element may optionally note products and versions that are no longer supported or are not affected by the vulnerability.

Information useful in describing affected products can include:

— product names, including common or historical names;

— version numbers or strings;

— file hashes;

— PoC code to safely test for the existence of the vulnerability.

7.4.7 Intended audience

Advisory authors should consider their intended audience when developing and producing the advisory. Typically, the audience will be users who are responsible for identifying vulnerable systems and performing remediation. Advisories may provide sections intended for specific audiences, for example, different remediation advice for developers, system administrators, or end users. Audience-specific language in an advisory is optional.

7.4.8 Localization

Vendors can provide advisories with appropriate language and localization selections.

7.4.9 Description

The advisory should provide sufficient information that users can establish if they are affected and to assess their exposure. At the same time, the advisory should not provide too much detail in order to avoid making exploiting the vulnerability easier.

Advisories may describe the class or type of vulnerabilities, for example using the CWE taxonomy.

7.4.10 Impact

The advisory should describe the potential impact or consequence of the vulnerability if it is exploited. The impact should at a minimum explain the direct technical behaviour that the vulnerability allows. The impact can describe security violations, access or privilege gains, likely subsequent impacts, and common attack scenarios.

The impact can be described using a model such as the CIA triad (confidentiality, integrity, and availability) or the Parkerian hexad (confidentiality, possession or control, integrity, authenticity, availability, and utility).

7.4.11 Severity

The advisory should provide a severity rating for each vulnerability to help users assess risk more quickly and programmatically. Advisory authors should consider existing systems such as CVSS, but may use other or develop their own systems. A severity rating system used in the advisory should be documented and the documentation referenced from the advisory.

7.4.12 Remediation

The advisory should provide information about what action affected users should take in order to remediate the vulnerability and reduce its impact. Remediation typically involves installation of an upgrade, patch, or new version.

As appropriate or necessary, the advisory should provide workarounds by which users can protect the affected product or service until a more permanent solution is implemented. Workarounds can include changing a product's configuration to restrict functionality and introducing a firewall to restrict network accessibility.

7.4.13 References

References to additional or related information may be added in this element. Examples of such references can be links to related advisories published by other parties or a reference to a CVE identifier. It is important to refer to original or source material and common cross-references such as CVE.

7.4.14 Credit

In this element, a vendor should acknowledge a reporter for reporting the vulnerability and being cooperative during the process, if the reporter wishes to be publicly credited. This is an optional element.

7.4.15 Contact information

The advisory should provide contact information so that readers of the advisory can contact the vendor.

7.4.16 Revision history

This element should contain the date when the advisory was first published. It may contain a modification history if the advisory is subsequently updated.

7.4.17 Terms of use

The advisory should provide information about copyright and terms of use and redistribution of the advisory.

7.5 Advisory communication

Vendors should establish and maintain appropriate methods for communicating advisories to their users. Common methods include web sites, mailing lists, feeds, and automatic update mechanisms. Each vendor may determine the best method as it applies to their user community. Vendors may also choose to post advisories to public vulnerability discussion forums to share their information with a wider audience.

Vulnerability databases monitor public disclosures and collect vulnerability reports. Contacting a database directly, disclosing in a monitored forum, or providing a stable and consistent distribution channel can lead to inclusion in vulnerability databases.

7.6 Advisory format

Advisories should be formatted consistently and in a manner that clearly conveys important information. Changes to the format will likely require readers to change tools and processes used to consume advisories. Therefore, changes should be made infrequently.

Advisory authors should consider providing the content in both human- and machine-readable formats such as CVRF. Machine-readable advisory formats should be documented.

7.7 Advisory authenticity

Vendors shall provide the ability to authenticate and verify the integrity of advisories. This can be accomplished by cryptographically signing the advisory. Accepting a counterfeit advisory and acting on it can cause systems to be compromised. Depending on the cryptographic technique used, a vendor should publish required cryptographic material or credentials (e.g. public keys or certificates).

7.8 Remediations

7.8.1 General

A primary purpose of advisories is to document remediations (see 7.4.10). An advisory may describe remediation activities. A remediation often takes the form of a software change.

7.8.2 Remediation authenticity

If users are required to take action to apply a remediation, then vendors shall provide the ability to authenticate and verify the integrity of remediations. Typically, this is implemented as digital signatures of software updates.

7.8.3 Remediation deployment

The mechanism used to deploy remediations should be tailored to match user needs and the way a product is operated in the field. Vendors should consider providing automatic update deployment systems that require limited or no user interaction. Vendors should provide a method to control the automatic update deployment systems if appropriate. Remediation deployment corresponds to the Release phase described in 5.6.6.

8 Coordination

8.1 General

Coordinators may play multiple roles in vulnerability disclosure, for example:

— act as a trusted liaison between involved parties;

— coordinate advisory public release dates;

— enable communication between primary stakeholders (vendors and reporters);

— enable controlled disclosure to other stakeholders (such as CSIRTs);

— provide experience and guidance to disclosure processes;

— provide domain-specific expertise;

— support and facilitate collaboration among stakeholders.

Coordinators should set appropriate expectations about the services and levels of support they provide. The choice of a coordinator may depend on such factors as geographical proximity, language and acceptable operation model.

In cases when there are multiple vendors affected by a vulnerability, vendors should attempt to coordinate the timing of release of their advisories, either directly or with the assistance of a coordinator. A vendor may request that the coordinator provide or obtain a CVE identifier. In some cases, more than one coordinator can be involved. Vendors may suggest that one coordinator act as a leader in order to reduce complexity and confusion.

8.2 Vendors playing multiple roles

8.2.1 General

After investigating a reported vulnerability, a vendor can find the need to act in the role of coordinator, reporter, or both. If a vulnerability is caused by some component or underlying platform which another vendor supplies, the initial vendor may act as a reporter or coordinator. In addition, vendors sometimes encounter situations where it is desirable for them to report vulnerabilities to other vendors, causing them to act in the role of a vulnerability reporter. This subclause describes how such vulnerability reporting among vendors should be carried out.

8.2.2 Vulnerability reporting among vendors

Typical cases when a vendor may report vulnerability information to other vendors include:

— when the vendor believes that a vulnerability in their product or service is caused by a component or a tool which they are licensed to use by the second vendor;

— when a vulnerability is identified with a new methodology or insight and many of other vendors' products and services of the same category are also believed to be vulnerable; or

— when a vulnerability is identified in a protocol or format supported by other vendors' products or services.

It may not always be possible for a vendor, reporter, or coordinator to identify all of the other affected vendors. Even in cases where the vendor can be identified, it may not be possible to identify an appropriate point of contact. Such cases can benefit from the involvement of a coordinator who can provide additional support to vendor contact and notification efforts.

8.2.3 Reporting vulnerability information to other vendors

A vendor can report vulnerability information to other vendors directly or indirectly through coordinators in the same manner that a reporter reports a potential vulnerability to a vendor. In this case, the initial vendor can also inform the other vendor when the vulnerability is interrelated with the initial vendor's product or service and request the other vendor provide remediation before public disclosure so that all the vendors involved can synchronize the disclosure.

9 Vulnerability disclosure policy

9.1 General

To convey intentions and expectations, vendors shall develop and publish an external vulnerability disclosure policy. Alternatively, a vendor may reference and adhere to an existing published policy. The policy shall contain the required elements in 9.2. The external policy is meant for reporters, users, and other stakeholders. A vendor may also create a corresponding internal policy. The internal policy is meant for employees or agents performing vulnerability disclosure for the vendor. The two policies

should agree. The internal policy can contain further details, private information, and processes that are needed for internal reasons and to meet the external policy.

Each vendor has different requirements and resources available for dealing with security vulnerability information. Vendors should develop policy before engaging in vulnerability disclosure. Developing a policy is part of the Preparation phase described in 5.6.2. The disclosure policy should state the intentions of the vendor, its responsibilities as well what the vendor expects from other stakeholders. The vulnerability disclosure policy should be simple and clear to facilitate easy reporting of vulnerabilities to the vendor. Vendors should consider intuitive placement of their disclosure policy and other relevant information. One such location can be a security web page (e.g., www.example.com/security).

9.2 Required policy elements

9.2.1 General

A vulnerability disclosure policy shall include the following elements.

9.2.2 Preferred contact mechanism

The provisions in 6.2.1 require that vendors provide one or more technically current and usable mechanisms to receive reports. Vendors shall include information about these contact mechanisms in the vendor's vulnerability disclosure policy.

Contact mechanisms can include one or more of the following:

a) e-mail address. Examples of e-mail aliases that can be used include the following:

   — security-alert@example.com;

   — security@example.com;

   — secure@example.com;

   — psirt@example.com;

   — csirt@example.com;

b) phone number;

c) web form. Advantages of this mechanism include greater ability to influence the content of reports (e.g., the vendor can distinguish between optional and mandatory information) and better integration with a vulnerability report database;

d) contact information for customer service, if customer service is trained to receive vulnerability reports.

9.3 Recommended policy elements

9.3.1 General

A vulnerability disclosure policy should include the following elements.

9.3.2 Vulnerability report contents

A vendor can wish to elicit information that might be helpful to understanding the vulnerability and possible remediation and mitigation. A vendor can provide a form for this purpose (see 6.2.1).

In cases when a vulnerability affects multiple vendors, it is useful for vendors to know if the reporter has also reported the vulnerability to the other affected vendors.

9.3.3 Secure communication options

Vendors should provide a secure communications channel using technologies such as TLS, S/MIME, or OpenPGP. If a vendor provides a web-based reporting mechanism, that mechanism shall use TLS (HTTPS) or an equivalent, widely-used cryptographic system that protects the confidentiality of submissions and authenticates the web site. Vendors should configure these capabilities prior to communication with reporters.

9.3.4 Setting communication expectations

Vendors should set expectations for communication, including initial acknowledgement and status updates. Vendors should provide updates to the reporter using the agreed method of communication.

It is important that vendors maintain open and cooperative dialogue with reporters so that information about vulnerabilities can be shared and risk for users can be reduced as efficiently as possible. If the vendor determines that the reporter has not provided enough information, the vendor may contact the reporter to request additional details. Vendors acting as reporters or coordinators communicate with other vendors in their supply chains. The policy should support all of these communications possibilities.

In most cases, the team dealing with vulnerability reports is not able to deal with security incidents and other security related questions. The policy may specify contact points for these other types of requests.

The policy may describe the mechanisms used to track reports and communications with reporters and other stakeholders.

9.3.5 Scope

Vendors should describe which products and services are eligible to receive remediations. Vendors should also describe which products and services are not eligible to receive remediations. For example, a product can be in a test phase or no longer supported.

9.3.6 Publication

Vendors should describe how advisories and remediations are distributed.

9.3.7 Recognition

Vendors should describe how reporters are recognized for their efforts. Recognition can include credit in advisories, gifts, and bounty payments.

9.4 Optional policy elements

9.4.1 General

A vulnerability disclosure policy may contain the following elements.

9.4.2 Legal considerations

The act of finding or reporting a vulnerability can violate law or other regulation. Vendors can consider not taking legal action against reporters who voluntarily, in good faith, report vulnerabilities.

9.4.3 Disclosure timeline

Vendors can publish expected timelines for response and disclosure.

Annex A
(informative)

Example vulnerability disclosure policies

A.1 Facebook

https://www.facebook.com/whitehat [1)]

A.2 CERT/CC

https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm [1)]

A.3 Zero Day Initiative

http://www.zerodayinitiative.com/advisories/disclosure_policy/ [1)]

A.4 Cisco

http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html [1)]

A.5 NCSC-FI

https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/vulnerabilitycoordination.html [1)]

https://www.viestintavirasto.fi/attachments/vulncoord/68RKIxXES/Vulncoord_policy_1.1.pdf [1)]

A.6 NCSC-NL

https://www.ncsc.nl/english/security [1)]

https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html [1)]

https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf [1)]

A.7 Rapid7

https://www.rapid7.com/disclosure/ [1)]

1) Retrieved on 2017-05-18.