INTERNATIONAL STANDARD

ISO/IEC 30111

Second edition
2019-10

Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Reference number
ISO/IEC 30111:2019(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, *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.

This second edition cancels and replaces the first edition (ISO/IEC 30111:2013), which has been technically revised. The main changes compared to the previous edition are as follows:

— a number of normative provisions have been revised or added (summarized in Annex A);

— organizational and editorial changes have been made for clarity and harmonization with ISO/IEC 29147:2018.

This document is intended to be used with ISO/IEC 29147.

Introduction

This document describes processes for vendors to handle reports of potential vulnerabilities in products and services.

The audience for this document includes developers, vendors, evaluators, and users of information technology products and services. The following audiences can use this document:

— developers and vendors, when responding to actual or potential vulnerability reports;

— evaluators, when assessing the security assurance afforded by vendors' and developers' vulnerability handling processes; and

— users, to express procurement requirements to developers, vendors and integrators.

This document is integrated with ISO/IEC 29147 at the point of receiving potential vulnerability reports and at the point of distributing vulnerability remediation information (see 5.1).

Relationships to other standards are noted in Clause 5.

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This document provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service.

This document is applicable to vendors involved in handling vulnerabilities.

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

3 Terms and definitions

For the purposes of this document, terms and definitions given in ISO/IEC 27000 and ISO/IEC 29147 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/

4 Abbreviated terms

The following abbreviated terms are used in this document.

CSIRT Computer Security Incident Response Team

PSIRT Product Security Incident Response Team

5 Relationships to other International Standards

5.1 ISO/IEC 29147

ISO/IEC 29147 shall be used in conjunction with this document. The relationship between the two is illustrated in Figure 1.

This document provides guidelines for vendors on how to process and remediate potential vulnerability information reported by internal or external individuals or organizations.

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.

While this document deals with the investigation, triage, and remediation of internally or externally reported vulnerabilities, ISO/IEC 29147 deals with the interface between vendors and those who find and report potential vulnerabilities.

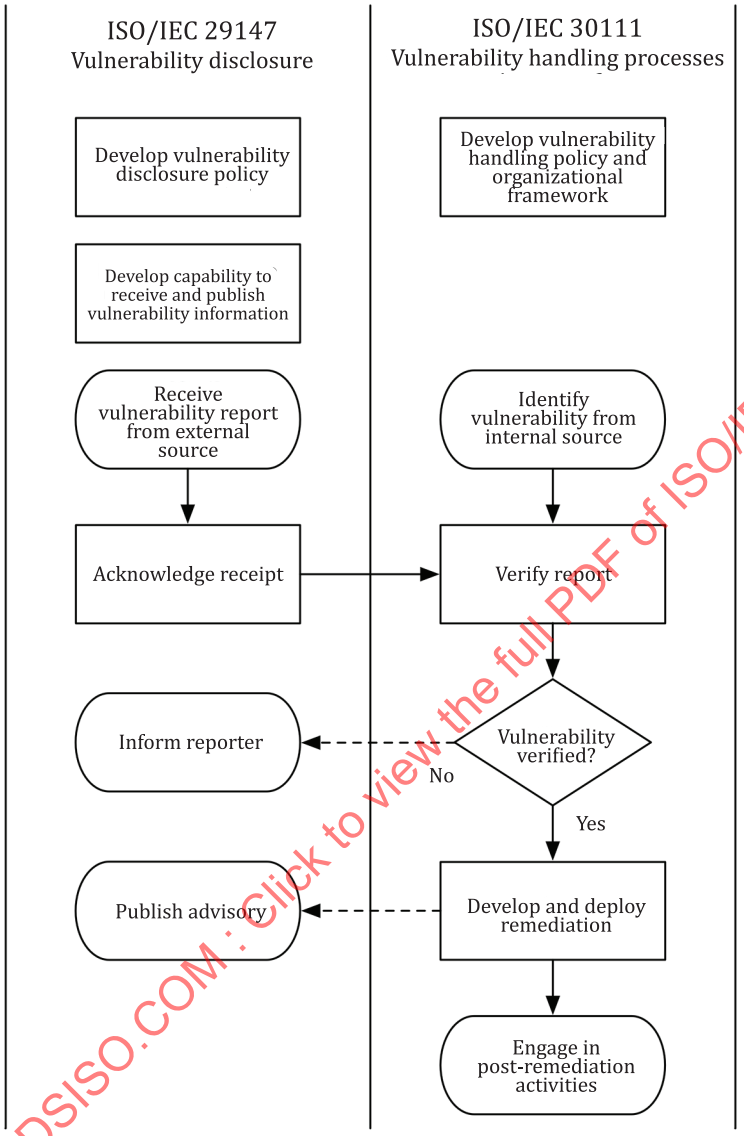

Figure 1 — Relationship between ISO/IEC 29147 and ISO/IEC 30111

5.2 ISO/IEC 27034 (all parts)

Application security seeks to reduce the creation of application vulnerabilities (see ISO/IEC 27034-1:2011, 6.5.2[1]). Application security techniques can also be useful for remediating reported vulnerabilities.

5.3 ISO/IEC 27036-3

Effective vulnerability handling processes require thorough understanding of ICT supply chain security as described in ISO/IEC 27036-3:2013, 5.4 a), 5.8 i), 6.1.1 a) 2) and 6.3.4[2].

5.4 ISO/IEC 15408-3

This document takes into consideration the relevant elements of ISO/IEC 15408-3:2008, 13.5[3].

6 Policy and organizational framework

6.1 General

Clause 6 describes the organizational elements that vendors should consider in their vulnerability handling processes. Vendors should create a vulnerability handling process in accordance with this document in order to prepare for investigating and remediating potential vulnerabilities. The creation of a vulnerability handling process is a task that is performed by a vendor and should be periodically assessed to ensure that the process performs as expected and to support process improvements. Vendors should document their vulnerability handling processes in order to ensure that they are repeatable. The documentation should describe the procedures and methods used to track all reported vulnerabilities.

See ISO/IEC 27034 (all parts)[1] for information on how identification of the root cause of a vulnerability, which is a step in the process of vulnerability handling, can help improve secure software development lifecycles and result in an outcome of more secure product development.

6.2 Leadership

6.2.1 Leadership and commitment

Top management should demonstrate leadership and commitment with respect to vulnerability handling by:

a) ensuring the policy and the objectives of vulnerability handling are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the vulnerability handling into the organization's processes;

c) ensuring that the resources needed for the vulnerability handling are available;

d) communicating the importance of effective vulnerability handling;

e) ensuring that the vulnerability handling process achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the vulnerability handling process;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

6.2.2 Policy

Top management should establish vulnerability handling policy that:

a) is appropriate to the purpose of the organization;

b) includes a best-effort commitment to satisfy user's requirements related to its product or online service security; and

c) includes a commitment to continual improvement of the vulnerability handling process.

More information about vulnerability handling policy is provided in 6.3.

6.2.3 Organizational roles, responsibilities, and authorities

Top management should ensure that the responsibilities and authorities for roles relevant to vulnerability handling are assigned and communicated.

Top management should assign the responsibility and authority for:

a) ensuring that the vulnerability handling process conforms to the requirements of this document; and

b) reporting on the performance of the vulnerability handling to top management.

6.3 Vulnerability handling policy development

A vendor shall develop and maintain an internal vulnerability handling policy to define and clarify its intentions for investigating and remediating vulnerabilities as part of a vulnerability handling process. This policy should be compatible with the external vulnerability disclosure policy required by ISO/IEC 29147.

The internal vulnerability handling the policy is intended for the vendor's staff and defines who is responsible in each stage of the vulnerability handling process and how they should handle reports about potential vulnerabilities. It should include the following items:

a) basic guidance, principles, and responsibilities for handling potential vulnerabilities in products or services;

b) a list of departments and roles responsible for handling potential vulnerabilities;

c) safeguards to prevent premature disclosure of information about potential vulnerabilities before they are fixed; and

d) a target schedule for remediation development.

The audience for the external vulnerability disclosure policy is internal and external stakeholders, including reporters who wish to report potential vulnerabilities, and users of the vendor's products or services. This policy informs the audience of how the vendor is willing to interact with them when a potential vulnerability is found in the vendor's product or services. Guidance, details and examples of public vulnerability disclosure policies are included in ISO/IEC 29147:2018, Clause 9 and Annex A.

6.4 Organizational framework development

Handling vulnerabilities has several additional aspects than just engineering and technology (for example, customer service and public relations). An organizational framework should be designed, recognized, and supported by the stakeholder divisions of the vendor responsible for each area.

An organization should have a role or capability that is responsible for and has authority to make decisions on vulnerability handling, preferably at a management level. This role or capability should understand the responsibility toward the vendor's users, the internal processes, and the organizational framework for vulnerability handling.

An organization should have a role or capability that is a point of contact for handling potential vulnerabilities. This point of contact should be identified for each division or department within a vendor that provides products or services to customers.

An organization should establish a point of contact for external parties to reach and communicate with about vulnerabilities. The point of contact can be part of a vendor computer security incident response team (CSIRT) or a product security incident response team (PSIRT). Further details are discussed in 6.5.

Since customers and members of the media can contact the vendor with questions or requests for additional information after a vulnerability is disclosed, divisions responsible for customer and public relations should be prepared so that they can respond.

6.5 Vendor CSIRT or PSIRT

6.5.1 General

Subclause 6.5 describes the organizational role and responsibilities of a CSIRT or PSIRT. For clarity, PSIRT will be used to refer to this role throughout the rest of this document. A PSIRT is responsible for coordinating external vulnerability reports. In some cases, a PSIRT also coordinates the handling of vulnerabilities that were reported by internal teams within the vendor.

6.5.2 PSIRT mission

A PSIRT plays a central role in a vendor's vulnerability handling processes. In addition to coordinating vulnerability handling internally, the PSIRT acts as a single point of contact for external stakeholders such as vulnerability reporters, coordinators, and other vendors.

Vendors should include all of their products and services in their vulnerability disclosure and vulnerability handling processes. A PSIRT should be implemented centrally within a vendor. However, a PSIRT may be implemented within a business unit, as long as all products and services are covered by the vendor's vulnerability handling processes.

6.5.3 PSIRT responsibilities

6.5.3.1 General

Subclause 6.5.3 describes the responsibilities of vulnerability response teams. This is an unordered list.

Example PSIRT services and functions can be found in the FIRST PSIRT Services Framework[4].

6.5.3.2 Public vulnerability monitoring

A PSIRT should monitor known public sources of vulnerability information for disclosures or discussion that affect the vendor's products or services. Sources can include mailing lists, social media, discussion forums, or vulnerability databases.

6.5.3.3 Communication with external reporters

A PSIRT should develop a single entry-point for receiving potential vulnerability reports from reporters or coordinators, typically either an e-mail address or a form on a web page.

A PSIRT is responsible for maintaining communication with reporters. It is important to understand the interests and motivations of reporters and to communicate in a timely manner.

A PSIRT may choose to handle security vulnerabilities from customers with a valid support contract through their customer support division rather than receiving them directly. In that case, appropriate processes and training should be provided to the customer support division. The customer support division should partner closely with the PSIRT to ensure that the vulnerability is appropriately handled and responded to.

For more information about communication with external vulnerability reporters, see ISO/IEC 29147:2018, 5.5.4 and Clause 6.

6.5.3.4 Communication within vendor organization

A PSIRT should work with product and services divisions to build a database of contacts for each product. When a potential vulnerability is reported, the PSIRT should identify the responsible product business division to dispatch the report to them through the contact person. The information should be shared confidentially on a need-to-know basis.

6.5.3.5 Communication with coordinators or other vendors

Where appropriate, a PSIRT should make arrangements for sharing vulnerability reports with coordinators or other vendors. They should be conscious of the vulnerability handling policy of the other party.

For more information, see ISO/IEC 29147:2018, 5.5.5 and Clause 8.

6.5.3.6 Timing of public vulnerability disclosure

A PSIRT should choose an appropriate date for each public vulnerability disclosure and prepare the advisory with the assistance of the product business division and other major stakeholders, such as legal, public relations, and external coordinators if applicable. The vulnerability disclosure should align to when the remediation is available so that users can take the necessary action.

For more information, see ISO/IEC 29147:2018, 5.6.8 and 7.3.

6.5.3.7 Internal vulnerability assessment

A PSIRT may test or coordinate testing of the vendor's own products or services for vulnerabilities and other security issues. Any vulnerabilities that are identified should be handled according to the vendor's vulnerability handling processes.

6.5.3.8 Inventory and supply chain tracking

A PSIRT should track the vulnerabilities found in all components used in the development of the vendor's products and services, including components from other business units or external suppliers. Vulnerabilities in third-party and shared components can affect the vendor's products and services.

Vendors should require software component inventory information from their suppliers. Such information can be provided as Software identification (SWID) tags defined by ISO/IEC 19770-2[5].

For more information, see ISO/IEC 29147:2018, 5.4.6 and 6.4.

6.5.4 Staff capabilities

The staff of a PSIRT should:

a) be able to understand the nature of reported potential vulnerabilities and coordinate with appropriate parties;

b) understand the confidentiality of vulnerability related information and be well-versed in handling such information in order not to leak the vulnerability details before remediation development;

c) notify an appropriate product business division to take actions necessary for vulnerability handling when appropriate.

6.6 Responsibilities of the product business division

A product business division provides customers with products or services that have been developed by the vendor or implemented and/or commercialized with other vendor's products or services. They are an entity responsible for a core part of handling process of vulnerabilities that affect their products or services.

When potential vulnerabilities are reported to a product business division by the PSIRT, the product business division should work with the PSIRT to develop remediations. Business divisions should have a means to escalate an issue to a PSIRT, if an issue is determined to be a vulnerability.

Product security contacts within business divisions should initiate the vulnerability handling process when they receive notification of potential security vulnerabilities in products or services. This process

should include notification of the PSIRT so that any necessary response actions are conducted as per the vendor's vulnerability response policies.

6.7 Responsibilities of customer support and public relations

Customer Support divisions should have the capability to handle and respond to security vulnerabilities reported by customers so that all customers are treated equally. Customer Support Division should partner closely with the PSIRT by following internally established processes to ensure that the vulnerability is appropriately handled and responded to.

In the final stages of vulnerability handling, advisories are often released with remediations. When the advisory is sent to customers via mailing lists or direct communications, the dissemination is often conducted by customer support divisions. Customer support should choose the appropriate means to inform all necessary customers and maintain confidentiality until the coordinated date of disclosure. See ISO/IEC 29147 for the timing of advisory release of multi-vendor vulnerabilities.

Some users can ask questions or request vendor support after reading the advisories. Customer support divisions should be prepared to respond to or escalate questions and requests concerning advisories.

As detailed in ISO/IEC 29147:2018, 7.5, advisories that are published on a vendor's public website should be easily accessible. Customer support or public relations divisions may be involved in the maintenance of the vendor's web site and should attempt to adhere to the guidelines in ISO/IEC 29147.

If a disclosed vulnerability is a serious or widespread issue, public relations divisions should prepare for contact from mass news media.

6.8 Legal consultation

Vendors can need legal review of proposed remediations and communications to ensure vendors are in compliance with internal policies, laws, and existing contracts.

7 Vulnerability handling process

7.1 Vulnerability handling phases

7.1.1 General

Figure 2 shows the phases within the vulnerability handling process. These phases give vendors a starting point from which to develop and organize their own specific vulnerability handling process. See also ISO/IEC 29147:2018, 5.6.

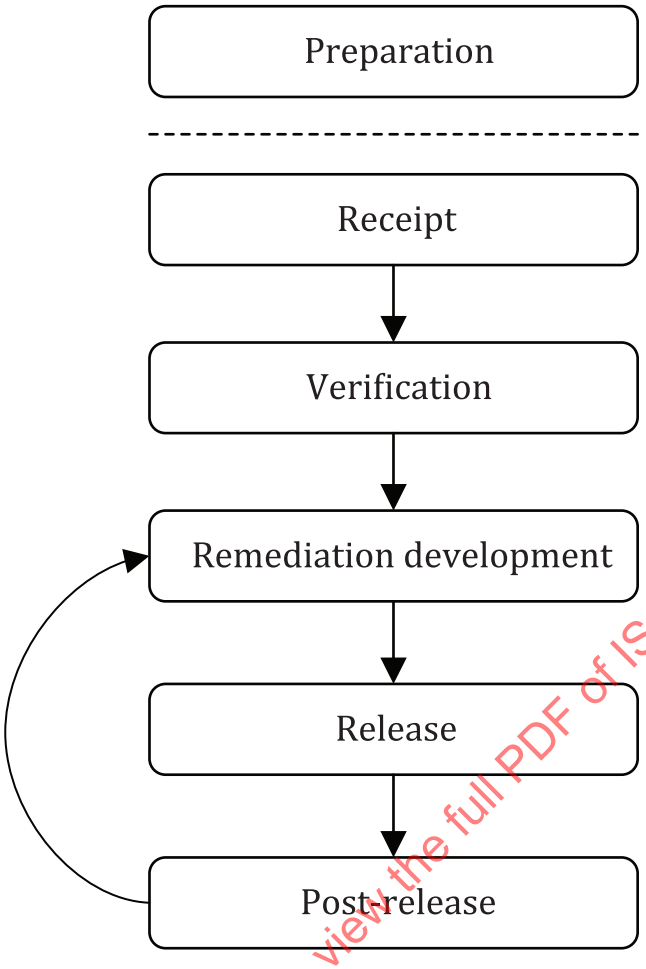

Figure 2 — Summary vulnerability handling process

7.1.2 Preparation

Vendors should develop policy (see 6.3), processes, and capability before starting a vulnerability handling program. In addition to other preparation activities, vendors may create a response organization (often called a PSIRT or CSIRT), create internal security assessment teams, hire and assign staff, and develop tools.

Vendors shall implement vulnerability disclosure process as defined in ISO/IEC 29147.

7.1.3 Receipt

The handling process for each vulnerability begins when receiving a new vulnerability report. Vulnerabilities reported to a vendor include:

a) internally found vulnerabilities and potential vulnerabilities: A vulnerability was discovered by the vendor during the development lifecycle or after product release;

b) externally found vulnerabilities and potential vulnerabilities: A vulnerability was discovered by a person or organization outside the vendor. See ISO/IEC 29147 for the interface with external vulnerability sources;

c) publicly disclosed vulnerabilities: A vulnerability was publicly disclosed without knowledge of and prior coordination with the vendor.

Records of all vulnerabilities and potential vulnerabilities received and processed by the vendor from any source should be maintained.

7.1.4 Verification

Vendors should verify reported vulnerabilities. The following steps may occur in parallel rather than sequentially.

a) Initial investigation: The vendor attempts to confirm the potential vulnerability, if the issue is found in a product or service that is supported by the vendor. Even if the potential vulnerability is reported in software or a service that is not currently supported, the investigation should continue until the vendor can determine whether the issue also affects supported products or services. The vendor determines the severity of the reported vulnerability.

b) Possible process exit: If the potential vulnerability cannot be verified or reproduced, then the vendor should ask the reporter for more information in order to attempt to successfully reproduce the issue. If more information is supplied, resume the investigation. Otherwise the vendor should exit the vulnerability handling process. If the potential vulnerability was discovered and reported by an external person or organization outside the vendor, then see ISO/IEC 29147 for communicating to the reporter the reason for terminating the process.

   Other circumstances can also cause the vendor to exit the vulnerability handling process without remediation, for example:

   1) Duplicate: The issue is a duplicate vulnerability and is already being addressed via this process or has already been remediated by the vendor.

   2) Obsolete product: The vulnerability is in a product that is no longer supported by the vendor.

   3) Non-security: The report either has no security implications or is not exploitable with currently known techniques. Vendors should note that exploitability can change when new techniques or attack vectors are discovered, so vendors should attempt to maintain awareness of current exploitation techniques. These reports may be addressed via the vendor's regular maintenance processes.

   4) Other vendor: The vulnerability is due to a product or service for which the vendor is not responsible. The vulnerability report should be passed to the responsible parties using the methods described in ISO/IEC 29147.

c) Root cause analysis: The vendor attempts to determine the underlying causes of the vulnerability and attempts to identify the affected products including all possible methods of exploitation as it relates to the instance of the vulnerability.

   As in 7.1.4 b) 4), if the vendor determines that the root cause is associated with products or services of another vendor, the vulnerability report should be passed to those vendors using the methods described in ISO/IEC 29147.

d) Further investigation: Attempts to find other instances of the same type of vulnerability in the product or service are made by the vendor. The investigation may extend to both earlier and subsequent versions of the product or service and may include other products and services produced by the vendor.

e) Prioritization: The vendor considers the threat posed by the vulnerability to affected users of the product or service. For each affected product or service, there can be different severities of the same underlying issue. The vendor should determine the severity of a vulnerability in the most commonly deployed conditions of affected products or services when possible to assist the prioritization. Vendors may consider several factors in determining the relative urgency of producing a remediation, such as potential impact, likelihood of exploitation, and the scope of affected users.

f) Inform the reporter of results of verification.

7.1.5 Remediation development

Vendors should develop and test remediations in the following sequential order.

a) Remediation decision: The vendor determines how the vulnerability can be remediated comprehensively, how to reduce the impact of successful exploitation of the vulnerability, or how to reduce exposure.

   When determining the best remediation, the vendor should attempt to balance the need to create a remediation quickly, with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues. In making this determination, the vendor should consider factors such as whether a vulnerability poses a high risk of exploitation of affected users, either due to the fact that it is simple to exploit, or due to the fact that the issue is already being actively exploited. A temporary or intermediary remediation that consists of a mitigation or workaround can be necessary in cases when a vulnerability poses a high risk to users. A non-comprehensive remediation that works in most scenarios can also be necessary in high-risk circumstances.

   The vendor should provide support to assist customers in dealing with vulnerabilities until a product has reached end of service. If vendor chooses not to remediate all supported versions, the vendor should attempt to provide a reasonable upgrade path from to a version that have remediations.

b) Produce remediation: The vendor produces patches, fixes, upgrades, documentation, or configuration changes to address a vulnerability. This step may also include the decision to inform a hosting subcontractor or the vendor's own web master to take vulnerable web pages offline, or to inform a publishing company to revoke a vendor's vulnerable application.

c) Test remediation: The vendor develops and performs appropriate tests to ensure the vulnerability issue has been addressed on all supported platforms. 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. If the remediation fails during testing, the vendor may alter or produce new remediations, iterating on the previous step in the process.

7.1.6 Release

The following list describes two possible paths a vendor can take to remediate a vulnerability. Typically, only one path is followed, but there are cases where elements of both scenarios can be needed to address a vulnerability. For example, a vendor that makes a change to their services on their own systems can also require that users change their passwords or log in and log out of the service, in order to fully remediate the vulnerability. The communication to users instructing them to take action would be handled via ISO/IEC 29147 in a security advisory issued by the vendor.

— Service vulnerability remediation: For vulnerabilities in services, vendors should follow their own update deployment or configuration change processes for production systems.

— Product vulnerability remediation: Once the vendor is satisfied that the vulnerability remediation is effective, the vendor should release the remediation using the processes defined in ISO/IEC 29147.

If the vulnerability was reported from an external party, then see ISO/IEC 29147 for the interface with external interested parties.

7.1.7 Post-release

Vendors should take the following actions in parallel after releasing the vulnerability remediation.

a) Case maintenance: After the remediation has been released, further updates to the remediation might continue. The vendor should update remediations as appropriate, generally until further

