INTERNATIONAL STANDARD

ISO/IEC 30111

First edition
2013-11-01

Information technology — Security techniques — Vulnerability handling processes

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

Reference number
ISO/IEC 30111:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 30111 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

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

The audience for this standard includes consumers, developers, vendors, and evaluators of secure IT products. The following audiences may use this standard:

— developers and vendors, when responding to reported actual or potential vulnerabilities;

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

— consumers, when selecting product and online service vendors to express best practice assurance requirements to developers, vendors and integrators.

This International Standard is related to ISO/IEC 29147.[5] It interfaces with elements described in ISO/IEC 29147 at the point of receiving potential vulnerability reports, and at the point of distributing vulnerability resolution information.

This International Standard takes into consideration the relevant elements of ISO/IEC 15408-3,[1] 13.5 Flaw remediation (ALC_FLR).

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This International Standard gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

This International Standard is applicable to vendors involved in handling vulnerabilities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

3 Terms and definitions

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

3.1
coordinator
optional participant that can assist vendors and finders in handling and disclosing vulnerability information

Note 1 to entry: Acts as trusted liaison between involved parties, enabling communication between involved parties (vendors and finders).

3.2
online service
service which is implemented by hardware, software or a combination of them, and provided over a communication line or network

EXAMPLE Search engines, online backup services, Internet-hosted email, and software as a service are considered to be online services.

3.3
product
system or service implemented or refined for sale or to be offered for free

Note 1 to entry: In information technology, a distinction is often made between hardware and software products, although the boundary is not always clear.

EXAMPLE A router can be seen as a hardware product even though a vital component of it is software and/or firmware.

3.4
remediation
patch, fix, upgrade, configuration or documentation change to address a vulnerability

Note 1 to entry: A change intended to resolve or mitigate a vulnerability. A remediation typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Remediations are usually provided by vendors. Vendors use different terms including update, patch, fix, hotfix, and upgrade.

3.5
service
means of delivering value to users by facilitating results users want to achieve without the ownership of specific resources and risks

3.6
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC 15288:2008, 4.31]

3.7
vendor
person or organization that developed the product, or service, or is responsible for maintaining it

3.8
vulnerability
weakness of software, hardware, or online service that can be exploited

[SOURCE: ISO/IEC 27000:2009, 2.46, modified]

Note 1 to entry: Examples of weaknesses in a system are software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems.

4 Abbreviated terms

CSIRT Computer Security Incident Response Team

PSIRT Product Security Incident Response Team

5 Interface between ISO/IEC 29147 - Vulnerability disclosure and ISO/IEC 30111 - Vulnerability handling processes

ISO/IEC 29147[5] - Vulnerability disclosure and ISO/IEC 30111 - Vulnerability handling processes are related standards, as Figure 1 shows. ISO/IEC 29147 provides a guideline for vendors to include in their normal business processes on receiving information about potential vulnerabilities from people or organizations externally and distributing vulnerability resolution information to affected users. ISO/IEC 30111 gives guidelines for how to process and resolve potential vulnerability information reported by individuals or organizations that find a potential vulnerability in a product or online service. While ISO/IEC 29147 deals with the interface between vendors and those who find and report potential vulnerabilities, ISO/IEC 30111 deals with the investigation, triage, and resolution of vulnerabilities, regardless if the source of the potential vulnerability was external to the vendor, or from within the vendor's own organization, typically security, development, or testing teams.

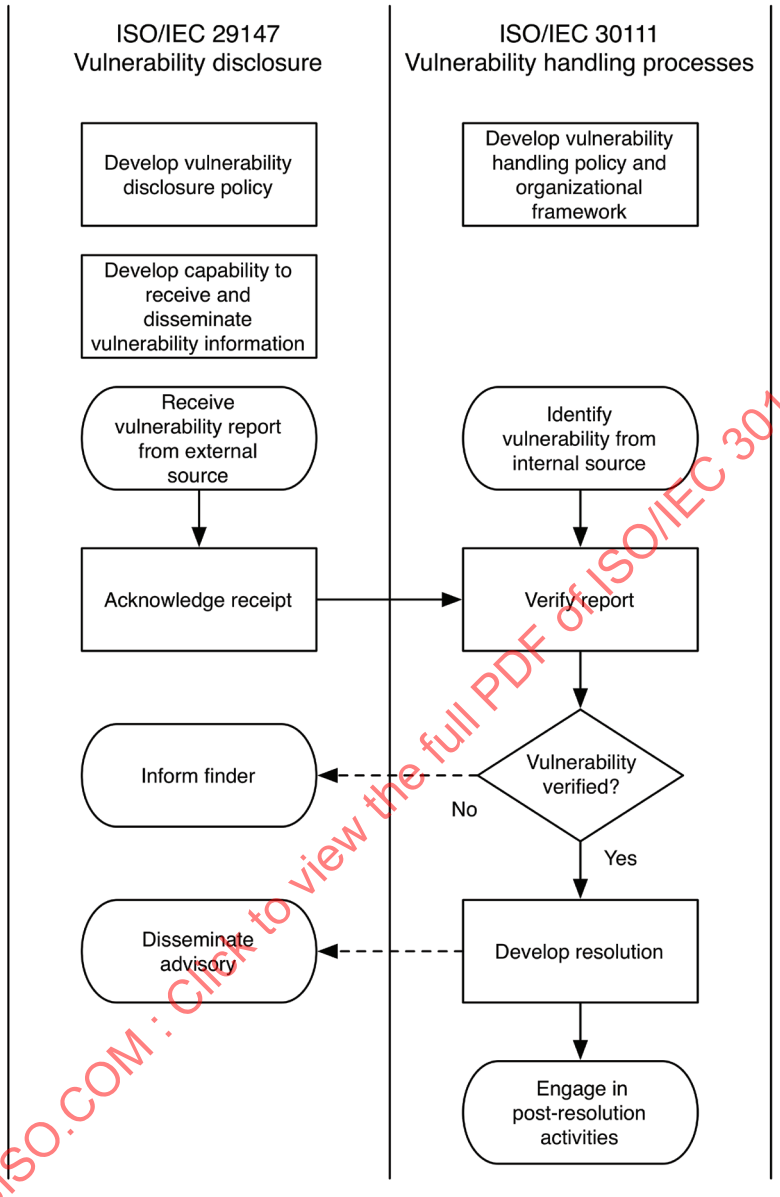

Figure 1 — A model of the Interface between ISO/IEC 29147 and ISO/IEC 30111

6 Policy and Organizational Framework for Vulnerability Handling Processes

6.1 General

Vendors should create a vulnerability handling process in accordance with this International Standard in order to prepare for investigating and resolving potential vulnerabilities. The creation of a vulnerability handling process is a task that is performed by a vendor, and should be periodically assessed to facilitate process improvement opportunities and ensure that the process performs as expected. Vendors should document their vulnerability handling procedure in order to ensure that it is repeatable. The documentation should describe the procedures and methods used to track all reported vulnerabilities.

See ISO/IEC 27034[3] 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. The following clause describes the elements that vendors should consider included in their vulnerability handling processes.

6.2 Vulnerability Handling Policy Development

A vendor should develop and maintain a vulnerability handling policy to define and clarify its intentions when investigating and remediating vulnerabilities for the development of a vulnerability handling process. The policy should consist of two parts: an internal-only portion and a public portion.

The internal-only part of 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 information on potential vulnerabilities. It should include the following items:

a) basic guidance, principles, and responsibilities for handling potential vulnerabilities in products or online 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.

The audience for the public part of the vulnerability handling policy is internal and external stakeholders, including finders who wish to report potential vulnerabilities, and users of the vendor's products or online services. It 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 online services. Guidance, details and examples of public vulnerability handling policies are described in the sections describing vulnerability disclosure processes in ISO/IEC 29147.[5]

6.3 Development of an Organizational Framework to Support the Vulnerability Handling Process

6.3.1 General

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 must 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 online 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 may be part of a vendor computer security incident response team (vendor CSIRT) or a product security incident response team (PSIRT). Its details are discussed in 6.4.

Since customers and members of the media may 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.

6.4 Vendor CSIRT or PSIRT

6.4.1 General

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

6.4.2 Vulnerability Response Team Mission

In vendor's vulnerability handling process, a vendor PSIRT plays a central role. In addition to coordinating vulnerability handling internally, it acts as a single point of contact for outside stakeholders such as finders of vulnerability and coordinators.

The function of a vendor PSIRT should be implemented centrally within the vendor, though it can be implemented within a product business division, if there is only a single product business division providing major products or online services from the vendor.

6.4.3 Vulnerability Response Team Responsibilities

6.4.3.1 General

This clause describes the responsibilities of vulnerability response teams.

6.4.3.2 Communication with external finders of potential vulnerabilities

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

A vendor PSIRT is responsible for maintaining communication with finders who reported potential vulnerabilities. It is important for vendors to understand the importance of timeliness, and finders' different agenda and stances on vulnerabilities.

6.4.3.3 Communication with product business divisions

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

6.4.3.4 Communication with coordinators or other vendors

Where appropriate, a vendor PSIRT shall make an arrangement for sharing vulnerability information with coordinators or other vendors. They should be conscious of the vulnerability handling policy of the other party.

6.4.3.5 Timing of vulnerability disclosure

A vendor PSIRT shall choose an appropriate date for each vulnerability disclosure and prepare the advisory with the assistance of the product business division and other major stakeholders, such as coordinators if applicable.

6.4.3.6 Public vulnerability monitoring

A vendor PSIRT should monitor known public sources of vulnerability information for disclosures or discussion that affect the vendors' products or online services. This may include open source forums or vulnerability databases.

6.4.4 Staff Capabilities

The staff of a vendor PSIRT should:

a) be able to understand the nature of reported potential vulnerabilities and dispatch them to 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 resolution development;

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

6.5 Responsibilities of the Product Business Division

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

When potential vulnerabilities are reported to a product business division by the vendor PSIRT, the product business division shall 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 and not a different type of bug.

Product security contacts within business divisions should initiate the vulnerability handling process when they receive notification of potential security vulnerabilities in products or online services. This process should include notification of the PSIRT so that any necessary response actions are conducted as per the vendors' vulnerability response policies.

6.6 Responsibilities of the Customer Support Division and Public Relation Division

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[5] for the timing of advisory release of multi-vendor vulnerabilities.

Some users may 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, 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 vendors' website 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.

6.7 Legal Consultation

Vendors may 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 Introduction to vulnerability handling phases

Figure 2 portrays a generic vulnerability handling process. Such a process is typically performed by the vendor.

The vulnerability handling process should require that a description of the nature and effect of each security flaw, and that the status of finding a correction to that flaw, be recorded.

A goal of a vulnerability handling process includes the provision of timely resolution to potential vulnerabilities.

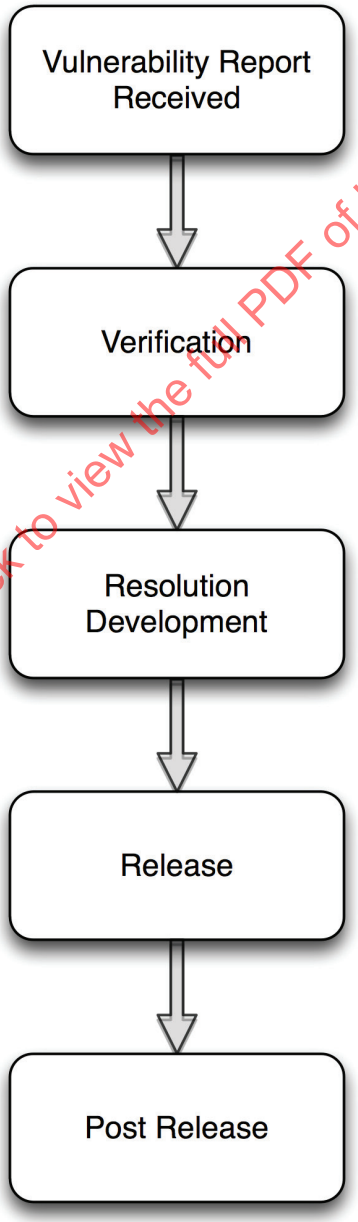

Figure 2 — A model of vulnerability handling

7.2 Vulnerability handling phases

7.2.1 General

This subclause describes the typical phases that occur when processing vulnerability reports. It provides a vendor a starting point to understand the related processes and permit the creation or modification of internal processes to deal with each situation as they arise.

7.2.2 Vulnerability report received

This sub-clause describes a vendor receiving a vulnerability report from either internal or external sources. Two sources may be considered:

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[5] for the interface with external vulnerability sources.

7.2.3 Verification

This subclause describes the verification of all kinds of vulnerabilities received. Records of all vulnerabilities and potential vulnerabilities received and processed by the vendor from any source should be maintained. During verification the following activities occur. Some of the following processes may occur in parallel, rather than sequentially, as described below.

a) Initial Investigation: The vendor attempts to confirm the potential vulnerability, if the issue is found in a product or online 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 either cannot be verified or reproduced, or the vendor determines that the issue is not considered a security vulnerability, then the vendor would exit the vulnerability handling process. If the potential vulnerability was discovered and reported by an external person or organization outside the vendor, then see also ISO/IEC 29147[5] that describes that vendors should ask the external entity more questions in order to attempt to successfully reproduce the issue before closing the investigation

   Other circumstances may also cause the vendor to exit the vulnerability handling process for the specific issue under investigation. If the issue was reported by an external person or organization outside the vendor, then see also ISO/IEC 29147[5] to communicate to the finder the reason to exit the process, among those below:

   1) Duplicate Bug: 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 Bug: The vulnerability is in a product that is no longer supported by the vendor.

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

4) Third-party Bug: The vulnerability is due to third-party code, configurations, or is present in a specification for which the vendor is not directly responsible. These issues should be passed to the parties who are responsible via 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.

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 online service. For each affected product or online service, there may 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 resolution, such as potential impact, likelihood of exploitation, and the scope of affected users.

7.2.4 Resolution development

This subclause describes developing a resolution for a vulnerability. The following steps should occur in sequential order.

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

When determining the best resolution, the vendor should attempt to balance the need to create a resolution quickly, with the overall testing required to ensure the resolution 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 resolution that consists of a mitigation or workaround may be necessary in cases when a vulnerability poses a high risk to users. A non-comprehensive resolution that works in most scenarios may also be necessary in high-risk circumstances.

b) Produce Remediation: The vendor produces patch(es), fix(es), upgrade(s), or documentation or configuration change(s) 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 page(s) 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.

7.2.5 Releasing the Vulnerability Resolution to the Next Stage in the Process

This subclause describes releasing a resolution for a vulnerability. If the vulnerability was reported from an external entity, then see ISO/IEC 29147[5] for the interface with external interested parties.

The following list describes two possible paths a vendor can take to resolve a vulnerability. Typically, only one path is followed, but there are cases where elements of both scenarios may be needed to address a vulnerability. For example, a vendor that makes a change to their online services on their own systems may 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.

a) Online service vulnerability resolution: For online services vulnerabilities, vendors should follow their own organizations' update deployment or configuration change processes for production systems.

b) Product vulnerability resolution: Once the vendor is satisfied that the vulnerability remediation is effective, it releases the remediation via the processes defined in ISO/IEC 29147.

7.2.6 Post Resolution Activities

This subclause describes vendor activities after releasing the vulnerability resolution. The items in this list can occur in parallel.

a) Case maintenance: After the resolution has been released, further updates to the resolution might continue. The vendor updates resolutions as appropriate, generally until further updates are no longer relevant, iterating on earlier phases in the vulnerability handling process, such as the Verification Phase or Resolution Development Phase.

b) Security development lifecycle feedback: The vendor updates the development lifecycle using information gained during the resolution process during root cause analysis to prevent similar vulnerabilities in new or updated products or services. See ISO/IEC 27034.[3]

c) Monitoring: In the case of resolving online services vulnerabilities, after the vendor applies the remediation, the vendor should monitor the stability of the product or service.

7.3 Monitoring of Vulnerability handling phases

Vendors should monitor the effectiveness of their vulnerability handling processes. This subclause describes aspects of the vulnerability handling process that should be monitored.

a) Speed: Vendors should monitor the time it takes to address a vulnerability through this process and strive toward improving the speed of vulnerability resolution. In case the risk level of the vulnerability is high, the rapid resolution of the vulnerability can help to limit the damage spreading.

b) Completeness: Vendors should monitor the completeness of the remediation, to ensure that it addresses the root cause of the vulnerability. The root cause analysis performed in the verification phase of the vulnerability handling process is critical to the completeness of the remediation. However, if urgency is required in order to address a vulnerability that is already being exploited, vendors may create a less complete remediation as a temporary measure and this should be taken into consideration when monitoring this aspect of the vulnerability handling processes.

c) Persistence: Vendors should monitor the remediation's effectiveness after it is released to affected users. It inspects how long the provided solution is being maintained to check the effectiveness of the solution for the vulnerability.

7.4 Confidentiality of Vulnerability Information

Vendors should take care to maintain the confidentiality of sensitive vulnerability information. There are two significant classes of information to protect. The first is personal or organizational identity information, such as the name of a finder who wishes to remain anonymous, or the IP addresses of a customer that has been compromised due to exploitation of a vulnerability. The second class is vulnerability information that is not yet published or widely known, such as a vulnerability that is still under investigation or technical details that inordinately benefit attackers.

Vendors should follow reasonable operational security practices to protect sensitive vulnerability information. These practices may include restricting access by organizational units and personnel on a "need-to-know" basis and encrypting data in transit over untrusted channels like email.

