

---

---

## Information technology — Security techniques — Vulnerability disclosure

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



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>Introduction</b>	<b>v</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Abbreviated terms</b>	<b>2</b>
<b>5 Concepts</b>	<b>3</b>
5.1 General	3
5.2 Interface between ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes	3
5.3 Products and online services	5
5.4 Stakeholders	6
5.5 Vulnerability disclosure process summary	7
5.6 Information exchange during vulnerability disclosure	8
5.7 Confidentiality of exchanged information	9
5.8 Vulnerability advisories	9
5.9 Vulnerability exploitation	9
<b>6 Vulnerability disclosure policy considerations</b>	<b>10</b>
6.1 General	10
6.2 Minimum policy aspects	10
6.3 Optional policy aspects	11
<b>7 Receipt of vulnerability information</b>	<b>12</b>
7.1 General	12
7.2 Potential vulnerability report and its secure receiving model	12
7.3 Acknowledgement of receipt from finder or a coordinator	12
7.4 Tracking incoming reports	12
7.5 On-going communication with finder	12
7.6 Detailed information	12
7.7 Support from coordinators	13
<b>8 Possible vulnerability reporting among vendors</b>	<b>13</b>
8.1 General	13
8.2 Typical cases calling for vulnerability reporting among vendors	13
8.3 Reporting of vulnerability information to other vendors	13
<b>9 Dissemination of advisory</b>	<b>14</b>
9.1 General	14
9.2 Purpose of advisory	14
9.3 Consideration in advisory disclosure	14
9.4 Timing of advisory release	14
9.5 Contents of advisory	15
9.6 Advisory communication	16
9.7 Advisory formats	17
9.8 Advisory authenticity	17
<b>Annex A (informative) Details for handling vulnerability/advisory information</b>	<b>18</b>
<b>Annex B (informative) Sample policies, advisories, and global coordinators</b>	<b>26</b>
<b>Bibliography</b>	<b>34</b>

## 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 29147 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

## Introduction

A vulnerability is a weakness of software, hardware, or online service that can be exploited. An exploitation of vulnerabilities results in a disruption of the confidentiality, integrity, or availability of the ICT system or related information assets, which may cause a breach of data privacy, interruption of operation of mission critical systems, and so on.

Vulnerabilities can be caused by both software or hardware design and programming flaws. Poor administrative processes and a lack of user awareness and education can also be a source of vulnerabilities, as can unforeseen changes in operating environments. Regardless of the cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems. Individuals and organizations, including businesses and governments, rely heavily on hardware and software components used in operating systems, applications, networks, and critical national infrastructure. Vulnerabilities in these components increase risk to the information residing on them, thus increasing risks to users and owners of the information. In addition, the lack of awareness about these vulnerabilities also increases risk.

Inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it. That is why vulnerability disclosure should be carried out appropriately.

Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability. It encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution.

The goals of vulnerability disclosure include the following:

- a) ensuring that identified vulnerabilities are addressed;
- b) minimizing the risk from vulnerabilities;
- c) providing users with sufficient information to evaluate risks from vulnerabilities to their systems;
- d) setting expectations to promote positive communication and coordination among involved parties.

This International Standard provides guidelines for vendors to be included in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.



# Information technology — Security techniques — Vulnerability disclosure

## 1 Scope

This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services. This International Standard details the methods a vendor should use to address issues related to vulnerability disclosure. This International Standard

- a) provides guidelines for vendors on how to receive information about potential vulnerabilities in their products or online services,
- b) provides guidelines for vendors on how to disseminate resolution information about vulnerabilities in their products or online services,
- c) provides the information items that should be produced through the implementation of a vendor's vulnerability disclosure process, and
- d) provides examples of content that should be included in the information items.

This International Standard is applicable to vendors who respond to external reports of vulnerabilities in their products or online services.

## 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 27000:2012, *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 in ISO/IEC 27000 and the following apply.

### 3.1

#### **advisory**

announcement or bulletin that serves to inform, advise, and warn about a vulnerability of a product

Note 1 to entry: An advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability at a specific point in time. An advisory can include a list of vulnerable products or services, potential impact, resolution and mitigation information, and references. Such items included in the advisory are relevant at the time the advisory is published and may evolve over time. An advisory may be published by a vendor, finder, or coordinator and may be revised if more information becomes available.

### 3.2

#### **coordinator**

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

Note 1 to entry: A coordinator can act as a trusted liaison between involved parties (vendors and finders), enabling positive communication between them.

**3.3  
finder**

individual or organization that identifies a potential vulnerability in a product or online service

Note 1 to entry: Finders can be researchers, security companies, users, governments, or coordinators.

**3.4  
online services**

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

Note 1 to entry: The vendor of an online service may also be referred to as a service provider. Online services are similar to products in that both are primarily software systems. Two main distinctions are that a service often appears to users as a single instance of software and that users do not install, manage, or deploy the software, but they only use the service.

**3.5  
product**

system implemented or developed for sale or to be offered for free

**3.6  
remediation**

patch, fix, upgrade, configuration, or documentation change to either remove or mitigate a vulnerability

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

Note 2 to entry: Actions that reduce the impact of a possible attack or mask the vulnerability (which are, in most cases, a temporary action) are often called countermeasures or workarounds.

**3.7  
service**

means of delivering value to users by facilitating results users want to achieve without the ownership of specific physical or logical resources and the risks related to ownership

**3.8  
vendor**

individual or organization that developed the product or service or is responsible for maintaining it

**3.9  
vulnerability**

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

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

Note 1 to entry: Weaknesses in a system can be caused by 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.

## **4 Abbreviated terms**

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System



ID	identifier
IT	information technology
PC	personal computer
PDF	portable document format
PGP	Pretty Good Privacy
PoC	proof of concept
PSIRT	product security incident response team
SRM	secure receiving model
SW	software
URL	uniform resource locator

## 5 Concepts

### 5.1 General

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

### 5.2 Interface between ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes

ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes are related standards, as [Figure 1](#) shows.

ISO/IEC 29147 provides guidelines for vendors to include in their normal business processes when receiving information about potential vulnerabilities from external individuals or organizations and when distributing vulnerability resolution information to affected users. This targets individuals, persons, users, and organizations who require methods to receive vulnerability reports and, when required, to disseminate advisories.

ISO/IEC 30111 gives guidelines on how to process and resolve potential vulnerability information reported by individuals or organizations that find a potential vulnerability in a product or online service. This is targeted at organizations who want to strengthen their internal processing to deal with received vulnerability reports.

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 security, development, or testing teams.

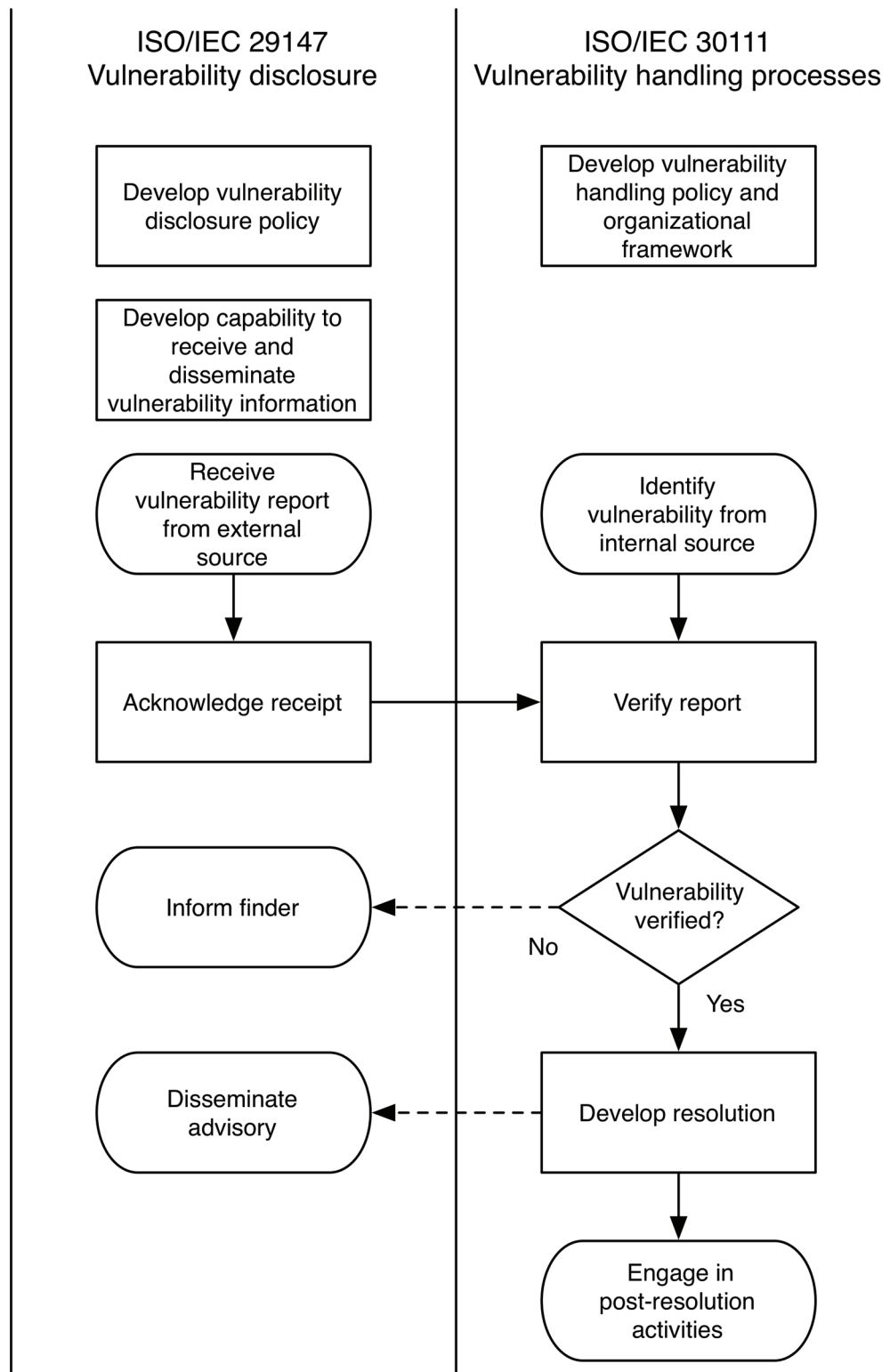


Figure 1 — Mapping of ISO/IEC 29147 and ISO/IEC 30111

## 5.3 Products and online services

### 5.3.1 Products

Products are systems provided by vendors to users either for sale or for free. There are many different types of products including but not limited to custom software built under contract for specific user's license 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.

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

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

### 5.3.2 Vulnerability

A vulnerability is generally a set of conditions that allows the violation of an explicit or implicit security policy of the user. Typically, the violation of the 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 might severely impact confidentiality and integrity since the attacker could 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 subjective factors.

Vulnerabilities are often caused by implementation defects in software. A vulnerability can be associated with 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 the Common Weakness Enumeration (CWE) and the Open Web Application Security Project (OWASP). Both of these organizations focus on training developers and engineers on current security threats including how to discover and rate them and how to programmatically make code and applications better. Links to both of these sites are located in [B.4](#).

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 and/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.

### 5.3.3 Product interdependency

Many products are complex systems that include other products in some way. Products can use source code from other products, software libraries, or other types of interfaces. Some products are substantially similar but sold under different brands by different vendors. Different products that support the same network protocol or file format may be affected by a vulnerability in the protocol or format. A user or

vendor may not be certain which products are affected by the vulnerability. These interdependencies are important since products that use or interact with a vulnerable product may also be vulnerable.

## 5.4 Stakeholders

This subclause enumerates major stakeholders in the vulnerability disclosure process.

### 5.4.1 User

Users may directly operate software or hardware products or make use of an online service. Users may be referred to as consumers, customers, or end users. Due to the interdependencies of modern software products, users may not know precisely which components or products they are actually using.

Users need information about vulnerabilities, particularly remediation, in order to make effective risk decisions and to use software products and online services more securely. Providing vulnerability information to users is discussed in [Clause 9](#).

### 5.4.2 Vendor

A vendor develops a product or online service or is responsible for maintaining it. A vendor may be an individual or organization such as a commercial business or an open source project. There are a number of different terms used to describe individuals or organizations who deliver software products for free, including developer, maintainer, or distributor. Similarly, an individual or organization that delivers software products within a supply chain may be called a supplier. For the purposes of this International Standard, the term “vendor” shall be used to mean all of them.

Vendors are responsible for the quality of their products and online services. Vendors use vulnerability disclosure to learn about vulnerabilities, to develop resolutions and mitigations, and to distribute information to users.

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. These intermediate vendors may be dependent on component vendors for vulnerability resolution and mitigation information.

### 5.4.3 Intermediate Vendor

An intermediate vendor gets a subsystem from a vendor and uses it to supply a system or service (or a combination of both) to a user (or another intermediate vendor). Typical examples are the following:

- a) system houses that use a PC and an operating system to add their own healthcare administration software and sell the combined system to a medical doctor (maybe together with a maintenance contract);
- b) telecommunication providers that supply a mobile phone together with a service contract.

These intermediate vendors may learn about vulnerabilities through error reports from their customers and additional early investigations (e.g. as part of quality controls for incoming goods). They shall report vulnerabilities to their vendors. The difficult issue for intermediate vendors is that they may not be in a position to simply wait for their vendor to solve the problem and remove the vulnerability.

They have a legal responsibility to inform their customers, as the customers may need to stop using the device or some of its functionality or to work around the vulnerabilities in order to mitigate risk. This holds especially when the vendor takes a long time to remove the vulnerability or is not able to do so at all. If an intermediate vendor informs its customer, this may well mean that vulnerability is disclosed before the vendor is able to deal with this.

Intermediate vendors may also be technically capable of producing and distributing workarounds to at least protect the use of their product or service or even a specific configuration of the underlying system (e.g. a more restrictive configuration of the operating system). Their intermediary role puts

these vendors in the position of having to deal with trade-offs (e.g. informing their customers about vulnerabilities quickly vs. communicating solutions in addition to problems).

#### 5.4.4 Finder

A finder is an individual or organization who identifies a potential vulnerability in a product or an online service. A finder is often a security or vulnerability researcher. A finder may also be a user or vendor. For the purposes of this International Standard, it is expected that a finder will attempt to inform a vendor or coordinator about a vulnerability. In practice, a finder may choose not to attempt to inform a vendor or coordinator or the attempt may fail. Receiving vulnerability information from finders is discussed in [Clause 7](#).

#### 5.4.5 Coordinator

Coordinators may work with other coordinators to obtain help with domain expertise, language, time zone, and cultural barriers and to share effort. Some Computer Security Incident Response Teams (CSIRTs) provide vulnerability coordination services on an operational basis, and other CSIRTs will help coordinate individual cases. Some vendors also provide coordination services.

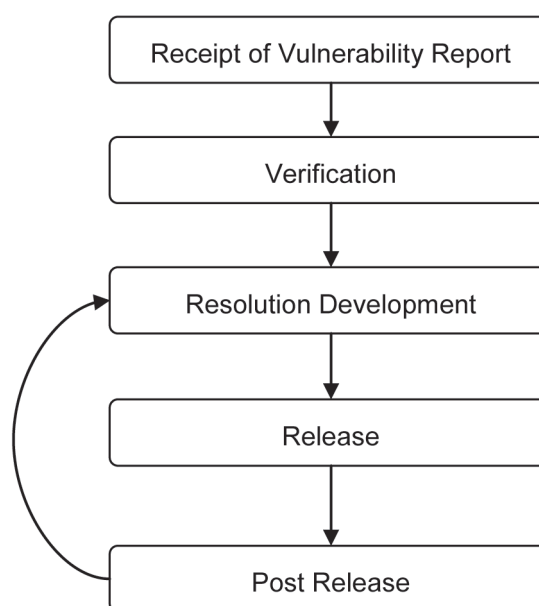
Common services provided by a coordinator include

- helping finders identify and contact vendors,
- coordinating vulnerabilities that affect multiple vendors,
- performing technical analysis and validation of vulnerability reports, and
- publishing advisories.

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

### 5.5 Vulnerability disclosure process summary

This subclause summarizes the vulnerability disclosure process contained in ISO/IEC 30111. [Figure 2](#) outlines the vendor's vulnerability disclosure process which consists of the five high-level steps.



**Figure 2 — Summary vulnerability disclosure process**

#### **5.5.1 Receipt of vulnerability report phase**

A finder identifies potential vulnerabilities in products or online services and reports to the vendor. The vendor acknowledges receipt of the report.

#### **5.5.2 Verification phase**

The vendor investigates the report. Investigation often involves attempting to reproduce the environment and behaviour reported by the finder. This may be a preliminary investigation, focused primarily on the need for further effort by the vendor. Investigation may 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 finder during the investigation and notifies the finder of the results at the end of the investigation.

#### **5.5.3 Resolution development phase**

The vendor develops a resolution for vulnerabilities reported by a finder. Resolution development may 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.

#### **5.5.4 Release phase**

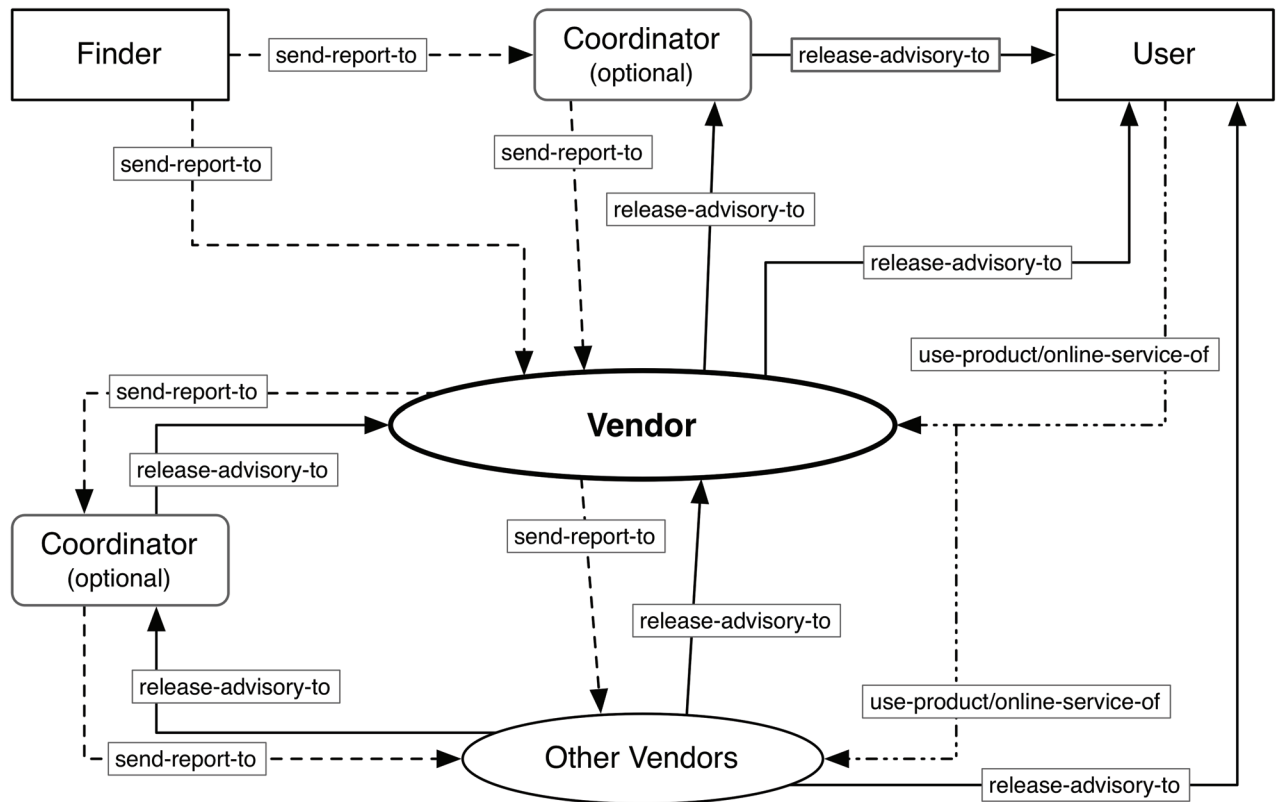
The vendor deploys the remediation. In an online service, the vendor deploys the remediation and documents the event. For a product, the vendor provides the remediation and mitigation information to users, typically in the form of a vulnerability advisory and software patches or updates, and users deploy the remediation. 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.

#### **5.5.5 Post-release phase**

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

### **5.6 Information exchange during vulnerability disclosure**

[Figure 3](#) illustrates information exchange during the vulnerability disclosure process. There are two main exchanges: potential vulnerability reports from finders to vendors and advisories from vendors to users. A potential vulnerability report is sent from a finder to a vendor either directly or through coordinators. A vendor may act as a finder and report a vulnerability to another vendor. An advisory is released by a vendor either privately to its users or to the public. This International Standard focuses on these two exchanges from the perspective of the vendor receiving vulnerability reports and disseminating remediation information.



**Figure 3 — Vulnerability information exchange**

## 5.7 Confidentiality of exchanged information

Since vulnerability information may be used to attack vulnerable products and online services, sensitive vulnerability information should be communicated confidentially. Vendors may wish to provide secure confidential methods for finders to report vulnerability information. Message integrity is also important, particularly in verifying that remediation information is authentic. Common cryptographic protocols such as Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), and Pretty Good Privacy (PGP) can provide confidentiality and integrity. If there are other security requirements, ISO/IEC 27010 may be of relevance. An example would be if a coordinator wishes to offer a finder anonymity service.

## 5.8 Vulnerability advisories

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

Users should be able to cryptographically verify the authenticity and integrity of an advisory and remediation (particularly patches and updates).

## 5.9 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 is fraught with uncertainty. The most conservative assumption is that a vulnerability can and will (and may have already been) used in attacks.



## 6 Vulnerability disclosure policy considerations

### 6.1 General

This clause discusses considerations to be taken into account when creating a vulnerability disclosure policy. Each vendor has different requirements and resources available for dealing with security vulnerability information.

Vendors should define their responsibilities in the vulnerability disclosure policy. Vendors should publicize their vulnerability disclosure policy or point to an existing public vulnerability disclosure policy. Several examples are listed in [B.1](#).

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 enable easy reporting of product vulnerabilities to the vendor. Vendors should consider intuitive placement of information related to product security. One such location may be a security web page (e.g. [www.example.com/security](http://www.example.com/security)).

### 6.2 Minimum policy aspects

A vendor should create an overall vulnerability disclosure policy, but they may choose to publicize only select sections if the internal policy contains sensitive information. A vulnerability disclosure policy should, at least, include information about the following.

a) How the vendor would like to be contacted

Vendors who adopt a policy of vulnerability disclosure will typically offer a security website or page. This website/page provides information on the vendor's accepted method(s) for receiving vulnerability information from a finder.

Contact information might include one or more of the following:

1) E-mail address;

Examples of e-mail aliases that could be used include the following:

- security-alert@example.com;
- security@example.com;
- secure@example.com;
- psirt@example.com;
- csirt@example.com

2) Phone number;

3) Web form.

Vendors can offer a web form that the finder has to complete. This has the advantage that the vendor can distinguish between optional and mandatory information and automate the process of entering data in a vulnerability database.

b) Secure communication options

Due to the risk aspect of clear text messages, vendors should provide a secure communications channel. This can leverage technologies such as S/MIME or PGP to ensure information exchanges are protected. Likewise, vendors can offer HTTPS for web portals for vulnerability report submissions. Vendors should configure these capabilities prior to communication with finders.

c) Setting communication expectations



Vendors should explain/set expectations for communication, including initial acknowledgement of receipt of report and status updates. Vendors should provide updates to the finder using the agreed method of communication.

d) Information that would be useful when submitting a possible vulnerability report

It is important that vendors maintain open and cooperative dialogue with finders so that information about vulnerabilities can be shared and risk for users can be reduced as efficiently as possible. Once a finder has initiated contact regarding a potential vulnerability, vendors will have to determine if the finder has provided enough information to confirm or refute the issue. This will be different in each situation. [A.2](#) lists examples of information that would be helpful to vendors. If the vendor determines that the finder has not provided enough information, the vendor may contact the finder to request for additional details. Intermediate vendors may wish to invite information on which terminal vendor or other intermediate vendor may be the source of the vulnerability and whether the finder also reported the vulnerability there.

e) Out-of-scope services

In most cases, the team dealing with vulnerability reports will not be able to deal with security incidents and other security related questions. Vendors should specify contact points for these types of requests.

A vendor may wish to provide suggestions for submitting additional information that might be helpful to understanding the vulnerability and possible remedies. The vendor might consider providing a form for this purpose.

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

f) How submitted reports are tracked

The vendor should define a means to track received information about possible vulnerability information and communicate that method with finders.

### 6.3 Optional policy aspects

A vulnerability disclosure policy may contain multiple optional elements.

a) Credit to finder

A vendor may acknowledge the contributions of the finder(s) who helped in the discovery or worked towards resolution of the discovered vulnerability. Before doing so, the vendor should verify that this acknowledgement is welcomed by the finder.

b) Synchronized public disclosure

As soon as remediations are available, the vendor and finder may come to a common and synchronized public disclosure.

c) Distribution

The vendor will offer a means for publishing security advisories which may include a website, mailing list, etc., including information on how to subscribe and unsubscribe.

## **7 Receipt of vulnerability information**

### **7.1 General**

This clause presents a guideline for vendors when receiving information on potential vulnerabilities from either a finder or a coordinator, which helps vendors

- a) ensure that their team responsible for vulnerability handling can receive vulnerability reports as quickly and securely as possible, and
- b) establish and maintain a working relationship with a finder or a coordinator.

### **7.2 Potential vulnerability report and its secure receiving model**

Potential vulnerability reports are sent to vendors or coordinators by finders in order to prompt initiation of the vulnerability handling process. They include a description of what product or online service has a potential vulnerability and how the potential vulnerability is triggered. Reports may include proof-of-concept (PoC) code that demonstrates the exploitation of the vulnerability. Since a vulnerability report may include sensitive information such as PoC code, a vendor should provide a means to receive that information securely.

### **7.3 Acknowledgement of receipt from finder or a coordinator**

The vendor should respond to a vulnerability report within the time period specified in the vendor's vulnerability disclosure policy. It is recommended that an acknowledgement of receipt of a vulnerability report be provided to a finder within seven calendar days.

### **7.4 Tracking incoming reports**

A vendor should have a tracking system that is used to record and track all reports on potential vulnerabilities. It shall be possible to unambiguously track each report. This assignment can be done by the vendor, an intermediate vendor, a finder, a coordinator, or any other party involved in the vulnerability disclosure process.

For tracking purposes, the vendor should assign a unique internal identifier to the potential vulnerability report. It is preferred to use this unique identifier in all communication with the stakeholders involved in the vulnerability assessment. Finders can also assign an internal identifier which can be included in the vendor's tracking process.

### **7.5 On-going communication with finder**

Vendors should evaluate the reported issue and make a determination whether it represents a vulnerability or not. The vendor should inform the finder and coordinator, if involved, on the results.

An intermediate vendor should check whether it can decide on the potential vulnerability on its own or needs to involve the vendor it got the related subsystem from. If another vendor needs to be involved in the decision and if this delays the response, the intermediate vendor should inform the finder and/or the coordinator about this fact and about the further processing.

### **7.6 Detailed information**

During the investigations, the vendor can lack sufficient information to come to a complete assessment of the vulnerability. In this case, the vendor should request that the finder provide additional input using the agreed upon communication channels.

Follow-up communication between the vendor and the finder will be conducted using agreed methods. One possibility is in web form. Examples of such web forms are shown in [A.3](#).

## 7.7 Support from coordinators

Coordinators can play the following multiple roles in the vulnerability disclosure process:

- a) act as a trusted liaison between involved parties;
- b) coordinate advisory public release dates;
- c) enable communication between involved parties (vendors and finders);
- d) provide an environment or forum where experts from different organizations can collaborate on addressing the vulnerability.

The choice of a coordinator can 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 can request that the coordinator provide or obtain a CVE identifier. In some cases, more than one coordinator can be involved. Vendors can suggest that one coordinator act as a leader in order to reduce complexity and confusion.

## 8 Possible vulnerability reporting among vendors

### 8.1 General

As a result of a detailed investigation of a reported vulnerability, a vendor can find it is caused by some component or underlying platform which another vendor supplies and whose vulnerability the vendor cannot resolve. In addition, vendors will sometimes encounter situations where it is desirable for them to report vulnerabilities to other vendors. This section describes how such vulnerability reporting among vendors should be carried out.

### 8.2 Typical cases calling for vulnerability reporting among vendors

Typical cases when a vendor can report vulnerability information to other vendors include the following:

- a) when the vendor believes that a vulnerability in their product or online service is caused by a component or a tool which they are licensed to use by the second vendor;
- b) when a vulnerability is identified with a new methodology or insight and many of other vendors' products and online services of the same category are also believed to be vulnerable;
- c) when a vulnerability is identified in a protocol or format supported by other vendors' products or online services.

Although the first vendor can identify other vendors to whom it should report the vulnerability information, it cannot be possible to do so in all cases. Even in cases where the vendor can be identified, it cannot be possible to identify an appropriate point of contact (e.g. in the case of open-source software). These cases can be handled effectively by requesting support from coordinators.

### 8.3 Reporting of vulnerability information to other vendors

A vendor could report vulnerability information to other vendors directly or indirectly through coordinators in the same manner that a finder reports a potential vulnerability to a vendor. In this case, the vendor might also inform them of the cases where the vulnerability is interrelated with its product or online service and request the other vendor provide a resolution before its public disclosure so that it can synchronize the vulnerability disclosure with the other vendor(s).

## 9 Dissemination of advisory

### 9.1 General

This clause discusses aspects of disseminating an advisory. Vendors at this stage have confirmed the presence of a vulnerability and are prepared to publish information to help affected users mitigate the associated risk.

### 9.2 Purpose of advisory

An advisory provides information about a vulnerability and should contain information about the risk based on successful exploitation and how to mitigate it.

### 9.3 Consideration in advisory disclosure

The following things should be considered when devising a process for producing and distributing advisories:

- a) Any party producing and distributing vulnerability information as an advisory should consider the needs of the intended audience. The content shall be appropriate and effective both in the informational content and distribution formats. Distribution formats are further described in [9.7](#).
- b) Users shall be able to verify the authenticity and integrity of an advisory. This can be accomplished by various means including cryptographically signing the advisory. Accepting a counterfeit advisory and acting on it can cause systems to be compromised.
- c) Ideally, an advisory and a remedy for a vulnerability are made available at the same time. However, special circumstances can arise when the vulnerability is being actively exploited and details of the vulnerability circulated. Under these conditions, a vendor can better serve its users by releasing an advisory bulletin or alert with possible workarounds (if such exist) rather than waiting until the remedy is produced.
- d) If a vulnerability affects multiple vendors or products, vendors should try to coordinate an advisory release such that it minimizes risk.
- e) Vendors should consider creating a mailing list to which interested parties can subscribe. This would include adding the necessary links on the vendor website and a posted policy.
- f) In order to help advisory consumers with assessing relative impact of different vulnerabilities, vendors should consider using a vulnerability severity scoring system, such as CVSS.
- g) A public database that represents a trusted repository for detailed and current vulnerability related information can be leveraged. These are offered by both public and private sources and, in some instances, can have a cost component to access the information.

### 9.4 Timing of advisory release

Vendors should work to balance risk when timing their advisory release. If no remediation exists for a vulnerability but attacks are underway, then a vendor may have to release an advisory to inform users of the risks and steps they can take to minimize or eliminate that risk. Otherwise, vendors should release advisories at the same time that remediation is available. If the vulnerability is not actively exploited by attackers, it is desirable to issue the advisory and the resolution promptly after it becomes available. However, when multiple advisories with the same product or online service are related, it is better to issue them at the same time to reduce the number of operation interruptions these collective resolutions can cause.

When a vulnerability is being actively exploited by attackers or a vulnerability is released to the public either intentionally or unintentionally, the responsible vendor should consider a prompt advisory with a

workaround or tentative resolution. This might result in a short-term solution until a patch or fix can be provided. In this situation, the advisory should be updated to provide the following most current details:

- a) vendors should, when possible, attempt to coordinate advisory release in instances where their products are affected by interrelated vulnerabilities. Releasing the information about the vulnerability in one product can expose other interdependent products to a higher risk of an attack. This situation will typically arise when a shared software library, protocol, module, or other component is utilized in multiple products or online services. The use of a coordinator would permit for controlled release and reduced risk to users. When considering aspects of a multi-vendor vulnerability, the readiness of customer support staff of call centres and sales divisions and other aspects should be considered.
- b) finder's agenda for publication.
- c) prevalence of activities exploiting the vulnerability.
- d) advisory release schedule of other vendors (when it is a multi-vendor vulnerability).

## 9.5 Contents of advisory

### 9.5.1 General

Advisories published by vendors should contain sufficient information to be useful for the targeted audience, which can include system administrators, developers, decision makers, product managers, etc. It shall help them to decide if the advisory is relevant for them and how to deploy remediation.

Users of advisories have different needs that could be dependent on market segment or regulatory requirements. Professional technical users such as system integrators tend to require detailed information about the threats and workarounds. Consumers typically appreciate information on how to determine if they are using the affected products. It also helps when it contains plain language and easy-to-understand description(s) to fix the problem. It is recommended that the vendor analyse the expected user base, based on the nature of their products, and provide information in an appropriate focus and layout. Unless otherwise stated, the order of the sections does not indicate an ordered operation.

The following sections detail a list of items that should be contained in an advisory. The list of items is not exhaustive and the vendor can, depending on the circumstances, include additional information in the advisory.

### 9.5.2 Identifier

A unique identifier should be provided for each advisory in order for it to be easily referenced.

### 9.5.3 Title

It is recommended that the title of an advisory contain a reference to a product or some other description that is informative to the users so that readers of the advisory can quickly decide if the advisory is relevant for them.

### 9.5.4 Overview

The overview portion of the vulnerability report 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.

### 9.5.5 Affected products

This section of the advisory provides a list of known affected products and their versions. If relevant, it can contain instructions on how to verify the version of the product currently in use. In the majority of

instances, online services do not have version identifiers but can have a date when the last update/change was made.

### 9.5.6 Intended audience

The advisory should list who the advisory is targeting from a readership perspective.

### 9.5.7 Description

The advisory should provide sufficient information that legitimate 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.

### 9.5.8 Impact

The advisory should provide information describing the impact of the vulnerability (e.g. Denial-of-Service, code execution). Additionally, a severity rating system (e.g. CVSS) can be used to provide additional information to help users assess exposure to a given vulnerability.

### 9.5.9 Remediation

The advisory should provide information about what action the users should take in order to remedy or mitigate the vulnerability and its impact. It often involves installation of a software patch or an updated version for software products.

As appropriate or necessary, the advisory should provide a workaround by which the users can protect the affected product or online service until the designated solution is implemented. Typical workarounds include changing a product's configuration to restrict its functionality, introducing a firewall to restrict network reachability of the product instance, and so on.

### 9.5.10 References

References to additional or related information can be added in this section. Examples of such references can be links to related advisories published by other parties or a reference to CVE ID.

### 9.5.11 Credit

In this section, a vendor can acknowledge a finder for reporting the vulnerability and being cooperative during the process, providing that the finder wishes to be publicly credited.

### 9.5.12 Revision history

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

### 9.5.13 Contact information

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

### 9.5.14 Terms of use

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

## 9.6 Advisory communication

Vendors should establish and maintain appropriate methods for communicating advisories to their users. Common methods include websites, mailing lists, feeds, and automatic update mechanisms. Each

vendor can determine the best method as it applies to their user community. Vendors can also choose to post advisories to public vulnerability discussion forums to share their information with a wider audience.

### **9.7 Advisory formats**

A consistent format for the advisories should be maintained in order to improve understanding of an advisory. While changes to format should be made when required, they should not be too frequent as users can customize some of their processes around certain features of an advisory.

When creating an advisory, the advisory producers should consider providing the content in both human and machine-readable formats. Examples of human readable advisories are provided in [B.3](#).

### **9.8 Advisory authenticity**

Users shall be able to verify authenticity of an advisory. 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 items or credentials on its website (e.g. public keys or certificates).



## **Annex A** **(informative)**

### **Details for handling vulnerability/advisory information**

In order to help the vendor handle a vulnerability report, the vendor can request that the finder provide the following detailed information. The vendor can offer a website or other electronic means to submit this information.

The information required will differ based on the vendor solution and the affected application/service. The following information will be useful when submitting a report to a vendor.

#### **A.1 Product**

##### **A.1.1 COTS based**

- a) Product Name — common name used for the solution;
- b) Operating System — installed operating system;
- c) Version Number using the vendor nomenclature if possible — version number including major and minor release details, if possible;
- d) Technical Description — provide what actions were being performed and the result in as much detail as possible;
- e) Sample Code — if possible, provide the code that was used in testing to create the vulnerability;
- f) Finder's Contact Information — best method to reach finder;
- g) Other Parties Involved — if there are other parties;
- h) Disclosure Plan(s) — current plan to disclose;
- i) Threat/Risk Assessment — contains details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;
- j) Software Configuration — details of the computer/device configuration at time of vulnerability;
- k) Relevant information about connected devices if vulnerability arises during interaction. When a secondary device triggers the vulnerability, these details should be provided.

##### **A.1.2 Hardware based**

- a) Hardware Model using the vendor nomenclature if possible;
- b) Hardware Revision Number — can be obtained from the command line interface or other management interface;
- c) Technical Description — provide what actions were being performed and the result in as much detail as possible;
- d) Sample Code — if possible, provide code that was used in testing to create the vulnerability;
- e) Finder's Contact Information — best method to reach finder;
- f) Other Parties Involved — if there are other parties;



- g) Disclosure Plan(s) — current plan to disclose;
- h) Threat/Risk Assessment — contains details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;
- i) Software Configuration — details to computer/device configuration at time of vulnerability;
- j) Relevant information about connected devices if vulnerability arises during interaction. When a secondary device triggers the vulnerability, these details should be provided.

### **A.1.3 Cloud based**

- a) For online services vulnerabilities, time and date of discovery;
- b) For online services vulnerabilities, URL;
- c) For online service vulnerabilities, browser information including type and version;
- d) For online service vulnerabilities, input required to reproduce the vulnerability;
- e) Technical Description — provide what actions were being performed and the result in as much detail as possible;
- f) Sample Code — if possible, provide the code that was used in testing to create the vulnerability;
- g) Finder's Contact Information — best method to reach finder;
- h) Other Parties Involved — if there are other parties;
- i) Disclosure Plan(s) — current plan to disclose;
- j) Threat/Risk Assessment — contains details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;
- k) Software Configuration — details to computer/device configuration at time of vulnerability;
- l) Relevant information about connected devices if vulnerability arises during interaction. When a secondary device triggers the vulnerability, these details should be provided.

## **A.2 Vulnerability reporting form**

If possible, a vulnerability reporting form should be used to obtain the necessary information. The following are examples from CERT/CC and JPCERT.

### **A.2.1 CERT/CC vulnerability reporting form**

#### **Vulnerability Reporting Form**

We accept reports of security vulnerabilities and serve as a coordinating body that works with affected vendors to resolve vulnerabilities. If you believe you have found a security vulnerability that has not been resolved, please complete the following form. As our vulnerability disclosure policy explains, we send information submitted in vulnerability reports to affected vendors. By default, we will share your name with vendors and publicly acknowledge you in documents we publish. If you do not want us to share your name or publicly acknowledge you, select the appropriate responses below.

For additional information about the fields in this form, refer to the instructions. If you have any problems or want to use another format for submitting this report, contact us.

Please provide as much information as you can. When you are finished, submit your report using the button at the end of the form.

*Your Contact Information*

Provide contact information about yourself in case we have additional questions regarding this vulnerability report. This information is not required to report a vulnerability, but without it, we will be unable to contact you.

Name:

Organization:

Email:

Telephone:

Can we provide your name to the vendor?                      Yes      No

Do you want to be publicly acknowledged?                      Yes      No

### *Vulnerability Description*

Please describe the vulnerability;

This field is required.

Which system configurations do you believe are vulnerable?

Check here if you believe the vulnerability is being exploited.

Check here if an exploit is publicly available.

### *Impact of Exploiting this Vulnerability*

Describe the specific impact and how you would envision it being used in an attack scenario:

### *Vendor Contact Information*

Which of the following statements best describes your communication with the vendor or vendors?

I have not notified the vendor, and do not plan to.

I have not notified the vendor, but plan to.

I have already notified the vendor.

I represent the vendor of the vulnerable product.

The vendor has already acknowledged the vulnerability publicly.

Who is the vendor of the product that contains the vulnerability? If you have already contacted the vendor regarding this problem, please share that contact information and any tracking numbers with us. If multiple vendors are affected, list them and explain how they are affected in Additional Vendor Information.

Vendor Name:

Contact Name:

Contact Email:

Contact Phone:

Vendor Tracking ID:

### *Additional Vendor Information*

Provide any additional information about the vendor and your communications with them.

*Upload a File*

You can specify one (1) related file to send us:

*CERT Tracking IDs*

If you have one or more CERT Tracking IDs for this report, enter them here:

*Additional Comments*

You can provide any additional comments that you would like to include:

*Submit Report*

Thank you for taking the time to complete our vulnerability reporting form. Click the button below to submit your report.

**A.2.2 IPA and JPCERT vulnerability reporting form****a) Agreement on Vulnerability Handling Policy**

I accept (The reporter agrees) that IPA and JPCERT/CC would maintain and process the reported vulnerability information in accordance with their vulnerability related information handling guideline, which is announced on the IPA website.

(If not the case, IPA cannot receive and handle the vulnerability report.)

**b) Contact information of the finder****1) Contact information**

Address (with state-level accuracy instead of full address):

Affiliation:

Name (either full name or nickname):

E-mail address:

Phone number:

FAX number:

Other items except “name” are optional if one of e-mail address, phone number, and FAX number is available.

**2) Acceptable use of reporter’s information, choose one from the following.**

- i) The reporter agrees that IPA can send the reporter’s contact information to JPCERT/CC and the product vendor.
- ii) The reporter wants IPA to keep the reporter’s contact information in secret and to act as a proxy in possible communication with JPCERT/CC and the product vendor.
- iii) Reference to the reporter in acknowledgement of advisories.
  - I) In advisories by JPCERT/CC, choose one from the following two:
    - a. the reporter’s name and/or affiliation can be included;
    - b. the reporter’s name and/or affiliation shall not appear.
  - II) In advisories by product vendors, choose one from the following two:
    - a. the reporter’s and/or affiliation name can be included;

b. the reporter's and/or affiliation name shall not appear.

If the reporter's name can be included in advisories, please specify how it should be referred:

Reporter's affiliation in Japanese:

Reporter's affiliation in English:

Reporter's name in Japanese:

Reporter's name in English:

c) Vulnerability related information

1) Source of the information, choose one from the following three:

- i) Reporter itself;
- ii) Reporter's acquaintance;
- iii) BBS, blog, and so on (URL).

2) Product in which the vulnerability is found

- i) Product name:
- ii) Software version:
- iii) Patch and fix:
- iv) Language version:
- v) Deviation from standard configuration:
- vi) Product vendor's name:
- vii) Product vendor's URL:

Information about a minor version, patches installed, a service pack, and hot fixes should be included in "Patch and fix".

3) Anomalous behaviour caused by the vulnerability

4) Procedure for reproduction of the vulnerable condition

5) Probability of the reproduction, choose one from the following three:

- i) Always
- ii) Often
- iii) Rarely

Additional comments for reproduction condition (such as dependency on version, language, and so on).

6) Possible threat caused by the vulnerability

7) Workaround

8) PoC (Proof of Concept) code

- 9) Other comments from the reporter (including severity assessment)
- d) Global availability of the product, choose one from the following five:
- 1) The software was developed outside of Japan.
  - 2) The software was developed in Japan, and some products including it are distributed widely in overseas countries.
  - 3) The software was developed in Japan, and it has been also distributed in overseas countries.
  - 4) The software was developed in Japan, and the reporter does not know whether it has been distributed in overseas countries or not.
  - 5) Other (            )
- e) Have you (Has the reporter) already reported the vulnerability to any other party than IPA? Choose one from the following two:
- 1) Yes, I have.
    - Date of the report:
    - Identifier of the report:
    - Name of the party:
    - Name of its contact person:
    - E-mail address of its contact:
    - Phone number of its contact:
  - 2) No, I have not.
- f) Protocol for further communication. Do you (Does the reporter) want messages sent from IPA to be encrypted?
- Choose one from the following:
- Yes
- No
- Please attach the public key if the case.
- g) Other items which should be reported

### A.3 Content of an advisory

In addition to the advisory list provided in [9.5](#) this clause provides a more comprehensive list of fields that can be included in an advisory.

#### Overview

This advisory should provide a summary on the vulnerability first so that the users can understand the essential points quickly.

#### Vulnerable software

If possible, the advisory should provide a descriptive list of affected products and versions. This might also include an explanation of how to confirm the version of these products including the vendor nomenclature for naming and numbering.

### Unique identifier

Names can be confusing when dealing with vulnerability information. In some case, it can lead to interpreting the incorrect vulnerability and potentially result in a system compromise. It is, therefore, imperative that the advisory use both a unique numbering and naming convention. The current system being used by many sources include that of CVE/MITRE who uses the following format:

CVE-YYYY-#### where 'Y' denotes the year of disclosure

This system would include an international scheme that could be referenced to find a particular vulnerability number. This does not exclude the fact that a component might or might not have their own numbering and naming conventions. It allows both the component owner and the interested parties to determine the specific details of the vulnerability and ensures that potential misinterpretations are minimized.

Several methods for exchanging vulnerability information exist currently. For example:

- a) Unique Identifiers
  - 1) Common Vulnerabilities and Exposures (CVE) Identifiers and dictionary for security vulnerabilities related to software flaws;
  - 2) Common Configuration Enumeration (CCE) Identifiers and dictionary for system configuration issues related to security;
  - 3) Common Platform Enumeration (CPE) Identifiers and dictionary for platform/product naming;
- b) Scoring systems
  - 1) Common Vulnerability Scoring System (CVSS).

These methods can greatly aid in increasing the reach of the disclosed information to all interested parties and should be considered by vendors when releasing disclosures.

To foster automated information exchange and provide greater information consistency among vendors, vendors should consider including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) information as part of their advisories. Both of them are part of ITU-T recommendation X.1500 (Cybex).

In most instances, the CVE initiative does not issue CVE-identifier numbers directly but instead relies on certain mechanisms to handle newly emerging information that are eventually provided to CVE. Therefore, to receive a CVE-ID number, the vendor should do one of the following:

- a) contact one of the CVE Numbering Authorities (CNAs) listed in the link below, which will then include a CVE-ID number in its initial public announcement about your new vulnerability;
- b) contact an emergency response team such as CERT/CC, DOE-CIAC, CanCERT, etc.;
- c) provide the information to a vulnerability analysis team;
- d) provide the assigned number CVE or other to the finder.

A list of CNAs is located at <http://cve.mitre.org/cve/cna.html>.

Common Vulnerabilities and Exposures (ITU-T recommendation X.1520) is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration". The intention of the CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. By citing the CVE in an advisory, users can more easily distinguish which vulnerability is the subject of the advisory. More information on CVE is available at <http://cve.mitre.org>.

Common Vulnerability Scoring System (ITU-T recommendation X.1521) provides for an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0 to 10 and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting a common language of scoring IT vulnerabilities. More information on the CVSS is available at <http://www.first.org/cvss>.

### **Description**

To make sure that the users do not confuse the vulnerability with other vulnerabilities identified in the same product, the advisory should clearly explain the vulnerability specifying the name, the cause, and other available information.

### **Threats**

The advisory should provide information about known threats that relate to the vulnerability, (e.g. the existence of exploit or proof-of-concept code, discussion or evidence of incident activity).

### **Impact**

The advisory should describe potential/expected consequences of attacks against the vulnerability. Attacks can have multiple impacts (e.g. an attack against a buffer overflow vulnerability could cause a crash or execute code). Where possible, describe secondary impacts (e.g. a cross-site scripting vulnerability directly allows an attacker to inject content into a web page; however, the secondary impact can be the exposure of cookies or other authentication credentials).

### **Solution**

For product vulnerabilities, the advisory should provide information on how to install the fixed product, update and apply a security patch.

### **Workarounds**

The advisory should provide workaround information if the users can protect the affected products in use through operational effort or by limiting the use of it in some way without applying the security patch.

### **References**

If additional information on the vulnerability that the users could refer to is available, the advisory should provide the links as reference.

### **Credit**

Some software vendors provide credit to the contributor for discovering and reporting the vulnerability. Depending on the policy/practice of the vendor issuing the advisory, it should provide credit as appropriate.

### **Revision history**

The advisory should clarify the date on which the vulnerability and what was updated.

### **Contact information**

The advisory should provide contact information in case the vulnerability information is unclear or the security patch has caused some issue. When possible, the software revision, patch ID, fix number, date, etc. should be included to ensure the specific software has been correctly identified to the end user.

## **Annex B** **(informative)**

### **Sample policies, advisories, and global coordinators**

#### **B.1 Sample vulnerability disclosure policy**

The following sample policy can be used as is or used to build upon. It can be applied to both software and services-based vendors. The policies and statements below do not reflect legal guidance and it is recommended that any company that posts a policy seek legal advice to determine fit and alignment to local legislation and laws.

##### **Introduction**

<company name> is committed to resolving vulnerabilities to meet the needs of its customers and the broader technology community. This document describes <company name> policy for receiving reports related to potential security vulnerabilities in its products and services and the company's standard practice with regards to informing customers of verified vulnerabilities.

##### **When to contact the security emergency response team**

Contact the <company name> Computer Security Emergency Response Team (CSERT) by sending email to security-alert@<company domain name> in the following situations:

- You have identified a potential security vulnerability with one of our products;
- You have identified a potential security vulnerability with one of our services.

After your incident report is received, the appropriate personnel will contact you to follow-up.

To ensure confidentiality, we encourage you to encrypt any sensitive information you send to us via e-mail. We are equipped to receive messages encrypted using S/MIME. A copy of the certificate that can be used to send encrypted email can be found on our website with this policy.

The security-alert@<companyname.com> email address is intended ONLY for the purposes of reporting product or service security vulnerabilities. It is not for technical support information on our products or services. All content other than that specific to security vulnerabilities in our products or services will be dropped. For technical and customer support inquiries, please visit <link to company technical support site>.

<company name> attempts to acknowledge receipt to all submitted reports within seven days.

##### **Receiving security information from <Company Name>**

Technical security information about our products and services is distributed through several channels.

- a) <company name> distributes information to customers about security vulnerabilities via e-mail to <name and link to addressed used for contact>. In most cases, we will issue a notice when we have identified a practical workaround or fix for the particular security vulnerability though there can be instances when we issue a notice in the absence of a workaround when the vulnerability has become widely known to the security community.

As each security vulnerability case is different, we can take alternative actions in connection with issuing security notices. <company name> can determine to accelerate or delay the release of a notice or not issue a notice at all. <company name> does not guarantee that security notices will be issued for any or all security issues customers can consider significant or that notices will be issued on any specific timetable.



- b) Security-related information can also be distributed by <company name> to public newsgroups or electronic mailing lists. This is done on an ad hoc basis, depending on how <company name> perceives the relevance of each notice to each particular forum.
- c) <company name> works with the formal incident response community to distribute information. Many company security notices are distributed by regional CSERT at the same time that they are sent through company information distribution channels.

All aspects of this process are subject to change without notice, as well as to case-by-case exceptions. No particular level of response is guaranteed for any specific issue or class of issues.

#### **Disclaimer:**

**Use of the information constitutes acceptance for use in an AS IS condition. There are no express or implied warranties or assurances with regard to this information. Neither the author nor the publisher accepts any liability whatsoever for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.**

## **B.2 Advisory samples**

The following are some sample advisories. They should be referenced as a model of good content and detail to provide to users. The advisories cited here are only a summary. It is recommended that the provided links be viewed to get the complete advisory for reference.

### **B.2.1 Advisory example from Microsoft**

Microsoft Security Bulletin MS09-018 - Critical

Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055)

Published: June 9, 2009

Version: 1.0

General Information

Executive Summary

This security update resolves two privately reported vulnerabilities in implementations of Active Directory on Microsoft Windows 2000 Server and Windows Server 2003, and Active Directory Application Mode (ADAM) when installed on Windows XP Professional and Windows Server 2003. The more severe vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

This security update is rated Critical for all supported editions of Microsoft Windows 2000 Server, and rated Important for supported versions of Windows XP Professional and Windows Server 2003. For more information, see the subclause, Affected and Non-Affected Software, in this clause.

The security update addresses the vulnerability by correcting the way that the LDAP service allocates and frees memory while processing specially crafted LDAP or LDAPS requests.

**Recommendation.** The majority of customers have automatic updating enabled and will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install this update manually. For information about specific configuration options in automatic updating, see Microsoft Knowledge Base Article 294871.

For administrators and enterprise installations, or end users who want to install this security update manually, Microsoft recommends that customers apply the update immediately using update management software, or by checking for updates using the Microsoft Update service.

See also the section, Detection and Deployment Tools and Guidance, later in this bulletin.

View the full advisory at <http://www.microsoft.com/technet/security/bulletin/ms09-018.msp>

The following CVE's are related to the Microsoft advisory example.

### Active Directory Invalid Free Vulnerability - CVE-2009-1138

A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. An attacker who successfully exploits this vulnerability could take complete control of an affected system.

### Active Directory Memory Leak Vulnerability - CVE-2009-1139

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server and Windows Server 2003. The vulnerability also exists in implementations of Active Directory Application Mode (ADAM) when installed on Windows XP Professional and Windows Server 2003. The vulnerability is due to improper memory management during execution of certain types of LDAP or LDAPS requests. An attacker who successfully exploits this vulnerability could cause the affected server to stop responding.

## B.2.2 Advisory example from Cisco

Document ID: 111512

Advisory ID: cisco-sa-20100217-csa

<http://www.cisco.com/warp/public/707/cisco-sa-20100217-csa.shtml>

Revision 1.2

Last Updated 2010 February 19 1000 UTC (GMT)

For Public Release 2010 February 17 1600 UTC (GMT)

Contents:

Summary:

Affected Products:

Details:

Vulnerability Scoring Details:

Impact:

Software Versions and Fixes:

Workarounds:

Obtaining Fixed Software:

Exploitation and Public Announcements:

Status of this Notice: FINAL

Distribution:

## Revision History:

## Cisco Security Procedures:

## Summary:

The Management Center for Cisco Security Agents is affected by a directory traversal vulnerability and an SQL injection vulnerability. Successful exploitation of the directory traversal vulnerability can allow an authenticated attacker to view and download arbitrary files from the server hosting the Management Center. Successful exploitation of the SQL injection vulnerability can allow an authenticated attacker to execute SQL statements that can cause instability of the product or changes in the configuration.

Additionally, the Cisco Security Agent is affected by a denial of service (DoS) vulnerability. Successful exploitation of the Cisco Security Agent agent DoS vulnerability can cause the affected system to crash. Repeated exploitation could result in a sustained DoS condition.

These vulnerabilities are independent of each other.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100217-csa.shtml>.

## Revision 1.0

2010-February-17

Initial public release.

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>

Updated: Feb 19, 2010 Document ID: 111512

The following CVE's are related to the Cisco advisory example.

*Management Center for Cisco Security Agents Directory Traversal Vulnerability*

The Management Center for Cisco Security Agents is affected by a directory traversal vulnerability that can allow an authenticated attacker to view and download arbitrary files from the server that is hosting the Management Center for Cisco Security Agents.

This vulnerability is documented in Cisco Bug ID CSCtd73275 and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0146.

*Management Center for Cisco Security Agents SQL Injection Vulnerability*

The Management Center for Cisco Security Agents is also affected by an SQL injection vulnerability that can allow an authenticated attacker to execute SQL statements that can cause the Management Center for Cisco Security Agents to become unstable or modify its configuration. These configuration changes can result in modifications to the security policies of the end points. Additionally, an attacker can create, delete, or modify management user accounts that are found in the Management Center for Cisco Security Agents.

This vulnerability is documented in Cisco Bug ID CSCtd73290 and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0147.

*Cisco Security Agent Denial of service vulnerability*

Cisco Security Agent is affected by a DoS vulnerability that could allow an unauthenticated attacker to cause a system to crash by sending a series of TCP packets.

**NOTE** Only Cisco Security Agent release 5.2 is affected by the DoS vulnerability. The Windows and Sun Solaris versions of the Cisco Security Agent are not affected by the DoS vulnerability.

This vulnerability is documented in Cisco Bug ID CSCtb89870 and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0148.

### **B.2.3 Advisory example from US-CERT**

#### **National Cyber Alert System**

Technical Cyber Security Alert TA10-159A

Adobe Flash, Reader, and Acrobat Vulnerability

Original release date: June 08, 2010

Last revised: June 29, 2010

Source: US-CERT

#### **Systems Affected**

- Adobe Flash Player 10.0.45.2 and earlier 10.x versions;
- Adobe Flash Player 9.0.262 and earlier 9.x versions;
- Adobe Reader 9.3.2 and earlier 9.x versions; Adobe Acrobat 9.3.2 and earlier 9.x versions

Other Adobe products that support Flash can also be vulnerable.

#### **Overview**

According to Adobe, there is a vulnerability in Adobe Flash. This vulnerability affects Flash Player, Reader, Acrobat, and possibly other products that support Flash. A remote attacker could exploit this vulnerability to execute arbitrary code.

#### **I. Description**

Adobe Security Advisory APSA10-01 describes a vulnerability in Adobe Flash that affects Flash Player, Reader, and Acrobat. It can also affect other products that independently support Flash, such as Photoshop, Photoshop Lightroom, Freehand MX, and Fireworks.

An attacker could exploit this vulnerability by convincing a user to open specially crafted Flash content. Flash content is commonly hosted on a web page, but it can also be embedded in a PDF and other documents or provided as a stand-alone file.

As noted in APSA10-01, "There are reports that this vulnerability is being actively exploited in the wild against both Adobe Flash Player, and Adobe Reader and Acrobat."

Additional information is available in US-CERT Vulnerability Note VU#486225.

#### **II. Impact**

If a user opens specially crafted Flash content, a remote attacker can execute arbitrary code.

#### **III. Solution**

##### **Update Flash**

Adobe Security Bulletin APSB10-14 recommends updating to Flash Player 10.1.53.64 or 9.0.277.0. This will update the web browser plugin and ActiveX control, but will not update Flash support in Adobe Reader, Acrobat, or other products.

### **Update Reader and Acrobat**

Adobe Security Bulletin APSB10-15 recommends updating to Reader and Acrobat version 9.3.3 or 8.2.3. This will update Flash support in Adobe Reader and Acrobat.

To reduce your exposure to this and other Flash vulnerabilities, consider the following mitigation techniques.

### **Disable Flash in your web browser**

Uninstall Flash or restrict which sites are allowed to run Flash. To the extent possible, only run trusted Flash content on trusted domains. For more information, see *Securing Your Web Browser*.

### **Disable Flash in Adobe Reader and Acrobat**

Disabling Flash in Adobe Reader will mitigate attacks that rely on Flash content embedded in a PDF file. Disabling 3D and Multimedia support does not directly address the vulnerability, but it does provide additional mitigation and results in a more user-friendly error message instead of a crash. To disable Flash and 3D and Multimedia support in Adobe Reader 9, delete, rename, or remove access to these files.

### **Microsoft Windows**

"%ProgramFiles%\Adobe\Reader 9.0\Reader\authplay.dll"

"%ProgramFiles%\Adobe\Reader 9.0\Reader\rt3d.dll"

### **Apple Mac OS X**

"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/AuthPlayLib.bundle"

"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/Adobe3D.framework"

### **GNU/Linux (locations can vary among distributions)**

"/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"

"/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

File locations can be different for Adobe Acrobat or other Adobe products that include Flash and 3D and Multimedia support. Disabling these plug-ins will reduce functionality and will not protect against Flash content hosted on websites. Depending on the update schedule for products other than Flash Player, consider leaving Flash and 3D and Multimedia support disabled unless they are absolutely required.

### **Prevent Internet Explorer from automatically opening PDF documents**

The installer for Adobe Reader and Acrobat configures Internet Explorer to automatically open PDF files without any user interaction. This behaviour can be reverted to a safer option that prompts the user by importing the following as a .REG file:

Windows Registry Editor Version 5.00

[HKEY\_CLASSES\_ROOT\AcroExch.Document.7]

"EditFlags" = hex:00,00,00,00

### **Disable the display of PDF documents in the web browser**

Preventing PDF documents from opening inside a web browser will partially mitigate this vulnerability. If this workaround is applied, it can also mitigate future vulnerabilities.

To prevent PDF documents from automatically being opened in a web browser, do the following:

- a) Open Adobe Acrobat Reader;
- b) Open the Edit menu;
- c) Choose the Preferences option;
- d) Choose the Internet section;
- e) Uncheck the “Display PDF in browser” checkbox.

### **Disable JavaScript in Adobe Reader and Acrobat**

Disabling JavaScript provides some additional protection against attacks. Acrobat JavaScript can be disabled using the Preferences menu (Edit - > Preferences - > JavaScript; uncheck Enable Acrobat JavaScript).

### **Enable DEP in Microsoft Windows**

Consider enabling Data Execution Prevention (DEP) in supported versions of Windows. DEP should not be treated as a complete workaround, but it can mitigate the execution of attacker-supplied code in some cases. Microsoft has published detailed technical information about DEP in Security Research and Defence blog posts “Understanding DEP as a mitigation technology” part 1 and part 2. Use of DEP should be considered in conjunction with the application of patches or other mitigations described in this document.

### **Do not access PDF documents from untrusted sources**

Do not open unfamiliar or unexpected PDF documents, particularly those hosted on websites or delivered as email attachments. Please see Cyber Security Tip ST04-010.

## **IV. References**

- Security Advisory for Flash Player, Adobe Reader and Acrobat — <http://www.adobe.com/support/security/advisories/apsa10-01.html>
- Security update available for Adobe Flash Player — <http://www.adobe.com/support/security/bulletins/apsb10-14.html>
- Security updates available for Adobe Reader and Acrobat — <http://www.adobe.com/support/security/bulletins/apsb10-15.html>
- Adobe Laboratories — Flash Player 10 pre-release — <http://labs.adobe.com/technologies/flashplayer10/>
- US-CERT Vulnerability Note VU#486225 — <http://www.kb.cert.org/vuls/id/486225>
- Securing Your Web Browser — [http://www.us-cert.gov/reading\\_room/securing\\_browser/](http://www.us-cert.gov/reading_room/securing_browser/)
- Understanding DEP as a mitigation technology part 1 — <http://blogs.technet.com/b/srd/archive/2009/06/05/understanding-dep-as-a-mitigation-technology-part-1.aspx>
- Understanding DEP as a mitigation technology part 2 — <http://blogs.technet.com/b/srd/archive/2009/06/12/understanding-dep-as-a-mitigation-technology-part-2.aspx>
- CVE-2010-1297 — <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297>

-----  
Feedback can be directed to US-CERT.  
-----

Produced 2010 by US-CERT, a government organization. Terms of use

#### Revision History

June 08, 2010: Initial release

June 11, 2010: Added CVE ID, updated for APSB10-14

June 29, 2010: Updated for APSB10-15

Last updated June 29, 2010

### **B.3 Coordinators recognized globally**

The following is a non-exhaustive list of globally recognized coordinators at the time this International Standard was last updated.

CERT Australia — [www.cert.gov.au](http://www.cert.gov.au)

CERT/CC (Software Engineering Institute (SEI) CERT Program of Carnegie Mellon University) — [www.cert.org](http://www.cert.org)

CERT-FI (Finnish national Computer Emergency Response Team) — <http://www.cert.fi/en/>

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) — [www.jpcert.or.jp/english/](http://www.jpcert.or.jp/english/)

### **B.4 Additional References**

Common Weakness Enumeration (CWE) — provides a unified method to determine software weaknesses — <http://cwe.mitre.org>

Open Web Application Security Project (OWASP) — provides methods to understand and test for web application weaknesses — [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)



## Bibliography

- [1] ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*
- [2] ISO/IEC 15443-1:2012, *Information technology — Security techniques — Security assurance framework – Part 1: Introduction and concepts*
- [3] ISO/IEC 19770-1:2012, *Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance*
- [4] ISO/IEC 19791:2010, *Information technology — Security techniques — Security assessment of operational systems*
- [5] ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*
- [6] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*
- [7] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*
- [8] ISO/IEC 27035:2011, *Information technology — Security techniques — Information security incident management*
- [9] ITU-T X.1521 (04/2011), *Common Vulnerability Scoring System (ITU-T Recommendations)*
- [10] ISO/IEC 27010:2012, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*





