ISO/IEC JTC 1/SC 22/WG 23 N 0260

ISO/IEC JTC 1/SC 27 N8780, 1st CD 29147, Information technology -- Security techniques – Vulnerability disclosure

Date	25 June 2010
Contributed by	SC 27
Original file name	ISO-IECJTC1-SC27_N8780_1stCD_29147_20100610.pdf
Notes	

Committee Draft **ISO/IEC 1st CD 29147**	Reference number: ISO/IEC JTC 1/SC 27 **N8780**
Date: **2010-06-10**	Supersedes document SC 27 N8126

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-09-10** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC 1st CD 29147

Title: Information technology -- Security techniques – Vulnerability disclosure*

Project: 1.27.65 (29147)

* subject to JTC 1 endorsement on the project title change

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
Study Period	33rd SC 27/WG 3 meeting, Nov. 2006, Resolution 14 (N5390).		Call f. Contr (N5567).
Study Period (extended)	34th WG 3 meeting, May 2007, resolution 7 (N5782) & 19th SC 27 Plenary, May 2007, 31 (N5939).	CA contr. (N5654); UK contr. (N5658);	Call f. contr. (N5970)
	35th WG 3 meeting, Oct. 2008, resolution 11 (N6153)	SoContr. (N6048); Rapporter's report (N6163)	Text NWIP (N6319rev1)
NP 29147 **1st WD 29147**	36th WG 3 meeting, Apr. 2008, resolution 4, P8 (N6640); 20th SC 27 Plenary, Apr. 2008, resolution 2 (N6799).	SoV on NP (N6493); US contr. (N6531); JP Contr. (N6880).	Liaison to FIRST (N6637); DoC (N7227); Text f. 1st WD (N6646).
2nd WD 29147	37th WG 3 meeting, Oct. 2008, resolution 5 (N7088).	FIRST com. (N7599); FIRST liaison (N7619); SoCom. (N7599)	Liaison to FIRST (N7269) DoC (N7266); Text f. 2nd WD (N7267).
3rd WD 29147	38th WG 3 meeting, May 2009, resolution 4 (N7783); 21st SC 27 Plenary, May 2009; resolution 2 (N7777).	FIRST liaison (N7619); FIRST Com. (N7600); SoCom. (N7599).	Liaison to FIRST (N7788) DoC (N7799); Text f. 3rd WD (N7901).
4th WD 29147	39th WG 3 meeting, Nov. 2009, resolution 5 (N8115).	FIRST Com (N8060); SoCom. (N8027).	Liaison to FIRST (N7945) DoC (N8127); Text f. 4th WD (N8126).
1st CD 29147	40th WG 3 meeting, Apr. 2010, resolutions 5, 9, P3 (N8796); SC 27 resolution 1 (N8916).	FIRST liaison (N8528); SoCom. (N8672); BE com. (N8551); CA com. (N8694).	Liaison to FIRST (N8788); DoC (N8779); Text f. 1st CD (N8780).

1st CD Registration and Consideration

In accordance with resolution P3 (in SC 27 N8796) of the 40th SC 27/WG 3 meeting held in Melaka (Malaysia), 19th – 23rd April 2010, the attached document SC 27 N8780 has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is hereby circulated for a 3-month 1st CD LB closing by

2010-09-10

Secretariat, ISO/IEC JTC 1/SC27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: krystyna.passia@din.de, http://www.jtc1sc27.din.de/en

Reference number of working document: **ISO/IEC JTC 1/SC 27 N 8780**

Date: 2010-04-30

Reference number of document: **ISO/IEC 1st CD 29147**

Committee identification: ISO/IEC JTC 1/SC 27

Secretariat: DIN

Information technology – Security techniques – Vulnerability Disclosure

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

vulnerability disclosure

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E
X:\TA3\TG3-3\NA043\NA043_Sekretariate\JTC1_SC27\03_Projekte\PROJECT_admin\29147_Responsible_Vulnerability_Disclosure_Mar2008\03_01_1stCD_29147_201100610\N8780_1stCD_29147_20100610\ISO-IECJTC1-SC27_N8780_1stCD_29147_20100610.doc Basic template BASICEN3 2002-06-01

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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, Security techniques.

Introduction

A vulnerability is a weakness of software, hardware, or online service that can be exploited by a threat.

Vulnerabilities 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. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems.

Users, 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 users.

Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a vulnerability and its resolution.

The goals of responsible disclosure include:

1) Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties.

2) Minimize the risk to customers from vulnerabilities that could allow damage to their systems.

3) Provide customers with sufficient information for them to evaluate the level of security in vendors' products.

4) Provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology.

5) Minimize the amount of time and resources required to manage vulnerability information.

6) Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities.

7) Minimize the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistent and explicit disclosure practices. “

Through vulnerability disclosure, vendors can work together diligently with vulnerability finders and produce a timely resolution to reduce users’ risks associated with the vulnerability in accordance with their business strategy.

This International Standard provides a guideline for vendors on receiving information about potential vulnerabilities and distributing vulnerability resolution information toward accomplishing vulnerability disclosure.

Editors Note

During the editing sessions in Melaka, Malaysia we had a discussion about possibly creating two separate documents. The first one would focus on the policy aspects and a second as a operational guide to vulnerability disclosure. It is requested that NB’s provide comments to this concept; including which sections they believe would reside in each part.

Vulnerability Disclosure

1 Scope Information technology -- Security techniques

This International Standard addresses the disclosure of potential vulnerabilities in products and online services.

This International Standard

↓ provides guidelines for suppliers on how to receive information about potential vulnerabilities in their products or online services;

↓ provides guidelines for suppliers on how to disseminate resolution information about potential vulnerabilities in their products or online services;

↓ proposes a process that should be implemented by a supplier for handling vulnerability disclosure;

↓ proposes the information items that should be used as input to a supplier's vulnerability disclosure process;

↓ proposes the information items that should be produced through the implementation of a supplier's vulnerability disclosure process;

↓ proposes content that should be included in the information items; and

↓ gives guidelines for the format of the information items.

This International Standard is applicable to

↓ suppliers who want to address the disclosure of potential vulnerabilities in their products or online services;

↓ users of products or online services that want to understand how a supplier should address the disclosure of vulnerabilities; and

↓ anyone interested in the management of vulnerabilities.

Users of this International Standard should consult all applicable laws and regulations. Implementing the guidance in this International Standard does not imply compliance to any applicable regulatory requirements. Implementers of this International Standard are responsible for observing or referring to the applicable regulatory requirements.

This International Standard is not intended to be in conflict with any organization's policies, procedures, and standards or with any national laws and regulations. Any such conflict should be resolved before using this International Standard.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary

3 Terms and definitions

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

For the purposes of this document, the following terms apply.

3.1
acquirer
individual or organization that acquires or procures a product or online service from a supplier
NOTE 1 Adapted from ISO/IEC 12207:2008.
NOTE 2 The acquirer could be one of the following: buyer, customer, owner, purchaser.

3.2
advisory
announcement or bulletin that serves to inform, advise and usually warn users about a vulnerability of a product

NOTE A vulnerability advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references. An advisory may be published by a vendor, finder, or coordinator.

3.3
coordinator
an optional participant that can assist vendors and finders in managing and disclosing vulnerability information

NOTE Participation of a coordinator is optional

3.4
finder
individual or organization that finds a potential vulnerability in a product or online service

NOTE Subgroups include researchers, security companies, users, governments, and coordinators.

3.5
malware
software designed to infiltrate a computer system without the computer owner's informed consent

NOTE 1 This definition was adapted from Wikipedia http://en.wikipedia.org/wiki/Malware .
NOTE 2 The term originated from the combination of two words “malicious” and “software”.
NOTE 3 The term is a general term used by computer professionals to mean a variety of forms of damaging, intrusive, or annoying software or program code.
EXAMPLE A maliciously crafted document that contains hidden vulnerability exploit code would be called malware.

3.6
maintainer
individual or organization that performs maintenance activities on a product or online service

NOTE Adapted from ISO/IEC 12207:2008

3.7
online services
service which is implemented by hardware, software or a combination of them, and provided over a communication line or network

NOTE 1 The content being hosted can be of a proprietary nature
EXAMPLE Search engines, online backup services, Internet-hosted email, and software as a service are considered to be online services

3.8
operator
individual or organization that performs the operations of a product or online service
NOTE 1 Adapted from ISO/IEC 12207:2008.

NOTE 2 The role of operator and the role of user may be vested, simultaneously or sequentially, in the same individual or organization.

3.9
private customer notification
Editors Note: The editor requests that NBs provide a definition for this term

3.10
product
system implemented or refined for sale or to be offered for free

NOTE 1 In information technology, 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 although is uses software

3.11
public disclosure
Editors Note: The editor requests that NBs provide a definition for this term

3.12
remediate
patch, fix, upgrade, configuration or documentation change to address a vulnerability

NOTE A change intended to resolve or mitigate a vulnerability. An update typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Updates are usually provided by vendors. Vendor use different terms including patch, fix, hotfix, and upgrade.

3.13
service
means of delivering value to acquirers by facilitating results acquirers want to achieve without the ownership of specific resources and risks
NOTE 1 Adapted from ISO/IEC 20000-1:xxxx
NOTE 2 A service is generally intangible.
NOTE 3 Services may also be provided by a supplier to the service provider.

3.14
stakeholder
individual or organization having a right, share, claim or interest in the handling of potential vulnerabilities in a product or online service in such a way that it meets their needs and expectations
NOTE Adapted from ISO/IEC 12207:2008.

3.15
supplier
individual or organization or an that provides a product or service to an acquirer
NOTE 1 Adapted from ISO/IEC 12207:2008.
NOTE 2 An acquirer is a stakeholder that acquires or procures a product or service from a supplier. Other terms commonly used for an acquirer are buyer, customer, owner, or purchaser.

3.16
system
combination of interacting elements organized to achieve one or more stated purposes
[ISO/IEC 15288:2008]

3.17
user
individual or organization that benefits from a product or online service during its utilization

NOTE 1 Adapted from ISO/IEC 12207:2008.

NOTE 2 The role of user and the role of operator may be vested, simultaneously or sequentially, in the same individual or organization.

3.18
vendor
person or organisation that developed the product, or is responsible for maintaining it

Editors Note: The editor request comments on the usage of the term “supplier” in the place of “vendor”. The rational would be that “supplier” is the ISO/IEC definition that includes “vendor” this would align the document to use SC27 standard definitions in the document. Comments on this topic are requested.

3.19
vulnerability
weakness of software, hardware, or online service that can be exploited by a threat

NOTE 1 Adapted from ISO/IEC 27000:2009
NOTE 2 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.
NOTE 3 Vulnerabilities can be architecture flaws, coding errors, or other implementation errors, or insecure configuration. Vulnerabilities can also result from insufficient or incorrect security documentation, security awareness, or communication.

4 Abbreviated terms

CCE – common configuration enumeration

CPE – common platform enumeration

CSIRT – Computer Security Incident Response Team

CVE – common vulnerability enumeration

CVSS – common vulnerability scoring system

ID – identification

IT – Information technology

PDF – portable document format

PGP – pretty good privacy

POC – proof of concept

PSIRT – Product Security Incident Response Team

SRM – secure receiving model

URL – uniform resource locator

5 Concepts

5.1 Introduction

The purpose of this clause is to highlight and to help explain essential concepts on which this International Standard is based.

5.2 Products and online services

5.2.1 Introduction

This International Standard focuses on vulnerabilities that can be found in products and online services. The purpose of this clause is to introduce these and related concepts in order to clarify the context of the International Standard.

5.2.2 Systems

A system is a combination of interacting elements organized to achieve one or more stated purposes. In general, these systems are man-made, created and utilized to provide products or services in defined environments for the benefit of users and other stakeholders. These systems may be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities. This view is too wide for the purpose of this International Standard.

NOTE 1 ISO/IEC 15288, Systems and software engineering – System life cycle processes and ISO/IEC 12207, Systems and software engineering – Software life cycle processes, provides more background to systems.

The term operational system is sometimes used for the combination of personnel, procedures and processes integrated with technology-based functions and mechanisms, applied together in a defined operational environment.

NOTE 2 ISO/IEC TR 19791, Information technology – Security techniques – Security assessment of operational systems, uses the term in this way.

This International Standard uses the term system to include only the information technology (IT) aspects of the system.

NOTE 3 ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security, uses the term in this way.

Also, only systems consisting of hardware and software, together with user documentation, are in scope of this International Standard.

NOTE 4 ISO/IEC 15443, Information technology – Security techniques – A framework for IT security assurance, defines a system as a specific IT installation, with a particular purpose and operational environment. The limitation to a particular operational environment is not within the scope for this International Standard.

A system element is a member of a set of elements that constitutes a system. It is a discrete part of a system that can be implemented to fulfil specified requirements. This International Standard is also applicable to system elements.

5.2.3 Software

Software is programs and other operating information that can be used by a hardware component. For the purpose of this International Standard, procedures associated with the programs and operating information is not considered as part of the software. Software is often referred to as code.

EXAMPLE A spreadsheet program as used on a personal computer.

5.2.4 Hardware

For the purpose of this International Standard, hardware is physical components. Hardware can often be seen as a device.

EXAMPLES Keyboards, memory modules, central processing units, motherboards.

5.2.5 Products

Products are systems which are implemented or refined for sale or to be offered for free.

In information technology, distinction is often made between hardware and software products, although the boundary is not always clear.

EXAMPLE A router is often seen as a hardware device. This is however not correct, since it consists of hardware and software.

For the purpose of this International Standard, the term product includes any combination of hardware and software to form an IT product, and the user documentation.

5.2.6 Service

A service is a means of delivering value to acquirers by facilitating results acquirers want to achieve without the ownership of specific resources and risks. A service can be provided by, or in combination with, a system or product. A service is often associated with the performance of activities, work, or duties associated with a product.

NOTE ISO/IEC 20000 provides processes, requirements, and guidance to service providers for the delivery of managed services.

5.2.7 Online service

Services can be provided in various ways. Often, services are provided from a remote location. An online service is a service which is provided over an information network, often the Internet. User documentation is also considered part of the online service.

EXAMPLES E-mail, storage, web conferencing.

5.3 Vulnerabilities

In general, a vulnerability is a weakness of an asset or control that can be exploited by a threat, where a threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.

NOTE 1 See ISO/IEC 27000 for information related to these terms.

Within the context of an information system, ISO/IEC TR 19791:2006 defines a vulnerability as a flaw, weakness or property of the design or implementation of an information system (including its security controls) or its environment that could be intentionally or unintentionally exploited to adversely affect an organization's assets or operations.

For the purpose of this International Standard, a vulnerability is a weakness in a product or online service that can be exploited by a threat. A vulnerability is initially defined from the perspective of the acquirer or user of the product or service, and is measured against this stakeholder's security policy. Because of this, and the many aspects that influence a stakeholder's perception of the existence of a vulnerability, this International Standard refers to *potential vulnerability* until the supplier has verified its existence.

NOTE 2 A vulnerability is also a failure or defect in a product or online service. IEEE Std. 1044, *IEEE Standard Classification for Software Anomalies*, provides a uniform approach to the classification of software anomalies, and can thus be helpful in the classification of vulnerabilities.

This International Standard does not address the scenario or process during which the potential vulnerability was discovered by the finder. Finding a potential vulnerability should be handled within the finder's security incident processes. This International standard focuses on the actions and processes of the supplier to receive and address reported potential vulnerabilities.

NOTE 3 ISO/IEC 27005 provides guidelines on identifying vulnerabilities.

It is not the purpose of this International Standard to provide guidance for the finder on how to verify the origin of the potential vulnerability.

EXAMPLE 1 Products can be used to build another system. A vulnerability in the design and use of the system is not a vulnerability in any of the products or sub-systems used to build the system.

EXAMPLE 2 Within a system, a vulnerability in one of the components can be incorrectly reported as a potential vulnerability in another component.

EXAMPLE 3 A firewall and an IDS, bought from two different suppliers, are used by an organization as part of its information security system. The firewall makes provision for dynamic rule configuration by an external IDS. However, the firewall expects different commands than those given by the acquired IDS. This constitutes a vulnerability in the system, but neither the firewall or IDS vendor is responsible for resolving the issue.

5.4 Information security incident management

Although not within the scope of this International Standard, it is mentioned here for a better understanding of the events leading to the process proposed in this International Standard.

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. An information security event is an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of controls, or a previously unknown situation that may be security relevant.

NOTE 1 See ISO/IEC 27000 for information related to these terms.

Information security incident management is the processes used for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

NOTE 2 See ISO/IEC 27035, Information technology – Security techniques – Information security incident management.

NOTE 3 ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements and ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management provides more information on the requirements for incident management and the management of technical vulnerabilities in an information security management system.

NOTE 4 ISO/IEC 20000-1, Information technology - Service management - Part 1: Service management system requirements, provides more information on the requirements for incident management in a service management system.

5.5 Information items

5.5.1 Introduction

An information item is a separately identifiable body of information that is produced, stored, and delivered for human use. Information item content is information included in an information item, associated with a system, product or service, to satisfy a requirement or need.

An information item has to be consistent with an information item generic type. An information item type is a group of information items consistent with a pre-arranged set of generic criteria. The information items addressed in this International Standard are of type description and report.

NOTE ISO/IEC 15289, Software and systems engineering – Content of life-cycle information products documentation), specifies the purpose and content of systems and software life cycle information items. Although the focus is on life cycle process information items, the general concepts are applicable.

5.5.2 Potential vulnerability reports

Editors Note: The editor requests that NBs provide content for this section

5.5.3 Verification report

Editors Note: The editor requests that NBs provide content for this section

5.5.4 Vulnerability descriptions

Editors Note: The editor requests that NBs provide content for this section

5.5.5 Advisories

Editors Note: The editor requests that NBs provide content for this section

5.6 Stakeholders

5.6.1 Introduction

A stakeholder, for the purpose of this International Standard, as an individual or organization having a right, share, claim or interest in the handling of potential vulnerabilities in a product or online service in such a way that it meets their needs and expectations.

NOTE ISO/IEC 15288, Systems and software engineering – System life cycle processes and ISO/IEC 12207, Systems and software engineering – Software life cycle processes, provides more information on the roles of supplier, acquirer, user etc.

This International Standard identifies the following stakeholders:

↓ supplier;

↓ maintainer;

↓ user;

↓ finder; and

↓ coordinator.

This International Standard does not make a distinction between the organizations to which the stakeholders belong. Thus, the concepts and process are equally applicable to scenarios where one or more stakeholders are part of the same organisation, and where all applicable stakeholders belong to separate organizations.

EXAMPLE The finder and supplier can be within the same organization, or they can be different organizations.

5.6.2 Supplier

A supplier is an individual or organization that provides a product or service to an acquirer. It has become customary to use the word “vendor” instead of the word “supplier” for this role. However, the common understanding of the word “vendor” is a person or company offering something for sale. This limits the provision of a product or service to only the instance of selling it. The word “supplier”, as used in International Standards for system and software engineering, is a more general term that addresses all roles in the provision of a product of service. This International Standard uses the word “supplier”.

5.6.3 Maintainer

A maintainer is an individual or organization that performs maintenance activities on a product or online service. Often, the role of maintainer and supplier is vested within the same organization. If this is not the case, then it important to ensure that a potential vulnerability is reported to the correct organization.

5.6.4 User

A user is an individual or organization that benefits from a product or online service during its utilization. A user can benefit directly or otherwise from remediation details, without having to be the finder.

5.6.5 Finder

A finder is an individual or organization that finds a potential vulnerability in a product or online service.

Typically, finders are users of a product or online service. In this case, the finder did not set out to find a vulnerability, but discovered a potential vulnerability during normal use of the product or on-line service. Often, finders also include researchers, security companies and governments that specifically scrutinize a product or on-line server for the presence of vulnerabilities.

5.6.6 Coordinator

A coordinator is an optional participant in the process that can assist suppliers and finders in managing and disclosing vulnerability information.

5.7 Communication

5.7.1 Secure Receiving Model (SRM)

Vendors and finders should use generally/mutually accepted encryption mechanisms to protect vulnerability information in e-mail or other transit. Vendors may provide HTTPS web forms or portal site receive and track vulnerability reports. The Vendor should use the details of communications methods and available encrypted mail certificates in the vulnerability disclosure policy.

5.7.2 Early Release

When an exception to the vulnerability handling process occurs, such as the finder releases vulnerability information before the mutually-agreed date, or the vulnerability is being actively exploited, the vendor should define how it will handle these exceptions.

6 Vulnerability Handling by Vendors

6.1 General

This clause discusses the typical phases that occur when processing vulnerability reports, which may become advisories. 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.

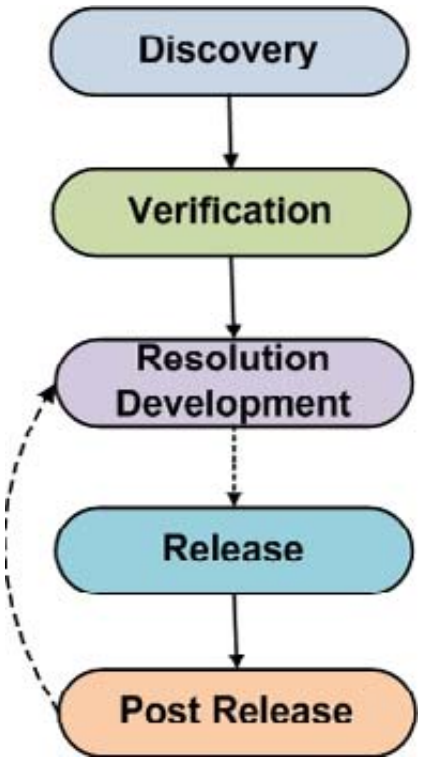

Figure 1. A Model of Vulnerability Handling by Vendors

a. **Discovery Phase**
   1. Discovery: A finder discovers a potential security vulnerability.
   2. Notification: The vendor is notified of the potential vulnerability either directly by the finder or through a coordinator. In some instances this might include a user provided malware sample for analysis.
   3. Acknowledgement: Vendors acknowledge receipt of the report.

b. **Verification Phase**
   1. Initial Investigation: The vendor attempts to confirm the vulnerability. The vendor, in possible co-operation with the finder, attempts to verify the submitted issue is a security vulnerability.
   2. Non-Vulnerability: If the potential vulnerability either cannot be verified or reproduced, or the vendor determines that the issue does not violate the security policy of the product, then the vendor should communicate the results of their investigation to the finder as part of the Resolution Phase. As part of the Verification Phase, the vendor should ask if the finder can produce further evidence that the issue is a security vulnerability before making their final resolution decision.
   3. Root Cause Analysis: The vendor attempts to determine 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.
   4. Further Investigation: Attempt to find other instances of the same type of vulnerability.
   5. Triage: Determine severity of the vulnerability.
   6. Exploit investigation: Attempt to determine whether the vulnerability has been exploited so far and how widespread the exploitation is.

c. Resolution Development Phase
   1. Action Point: Vendor determines how they will deal with the vulnerability.
   2. Produce Remedy: patch, fix, upgrade, or configuration change to address a vulnerability.

3. Test Update: perform a reasonable amount of test cases to ensure the vulnerability issue has been addressed. The vendor should attempt to ensure the remediation does not introduce new vulnerabilities.
4. Non-Vulnerability Remedy: If the vendor decides not to issue an advisory, either because they could not reproduce the issue or they disagree that the issue is a security vulnerability, the vendor should communicate this decision to the finder. The vendor would not execute subsequent phases of the lifecycle in this case.

d. Release Phase

1. Production system update: for online services vulnerabilities, implement the resolution in the production system.
2. Update Release: Once the vendor is satisfied that the update is effective, it notifies customers and possibly the general public via an advisory. Under extraordinary circumstances a vendor can release an advisory even if a remedy is not available.

e. Post Release Phase

1. Case Maintenance: After advisory has been released further updates to the advisory might continue. The vendor updates advisories as appropriate, generally until further updates are no longer relevant.
2. Feedback: Any new collateral effects, modifications of the malicious exploit, or new discoveries of the vulnerability or patch's effects on customer installations are fed back to the vendor that issued the patch. The reason could be that the vendor has confirmed with a high percentage of customers that affected software is patched; the affected software is obsolete; or the vulnerability and its solution are known for a long time. At this point, the case is considered closed.

These phases identify at a high level the tasks related to dealing with a potential vulnerability. They can be aligned to two primary functions: receiving and dissemination.

- Receiving deals with obtaining the details of the possible vulnerability.

- Dissemination aspect focuses on notifying affected parties.

The remainder of this document focuses on these aspects.

7 Vulnerability Handling Policy

7.1 General

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

7. 2 Policy Considerations

Vendors should define their responsibilities in the vulnerability handling policy. A policy should state the intentions of the vendor as it relates to vulnerability reporting. The vendor may choose not to have a detailed internal operational policy on the company's public portal. This might include contact information, timelines, communications channels, etc. It can be as open as the vendor is willing to operate. Vendor should publicize their vulnerability handling policy or point to an existing public vulnerability handling policy. Several examples are listed in Annex B.1 Sample Vulnerability Disclosure Policy.

A vulnerability policy should, as a minimum, include information about the following:

a. Keep the vulnerability handling policy simple

The vulnerability handling 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 management. Usage of security web page for this purpose is recommended.

b. How the vendor would like to be contacted

This can range from e-mail to toll free telephone numbers. This will really depend on the vendor and the degree of support they are able to allocate to this function. All vendors do not have the same resources and should write this section to match these capabilities. Once a vendor has created a contact for receiving vulnerability information, the vendor should publish the contact information on their website, and also should give their contact information to vulnerability coordinators. Vendors will do their best effort to provide their contact information to the coordinators.

c. Expected responses

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

d. Information that would be useful with submitting a possible vulnerability report

This will depend on the vendor and the nature of the solution they are providing. It would be helpful for finders to provide any information regardless of policy requirement. If the finder does not have the minimum it is better to get the finder to submit some aspects rather than no information.

Making a statement that clearly articulates the ability to submit information without a full technical disclosure will still be helpful in most cases.

e. Opening a vulnerability handling case

A unique identifier, typically a number should be assigned to the vulnerability as soon as possible in the disclosure process. This can be done by the vendor, finder, coordinator, to all parties involved in the responsible disclosure process. It is possible that two identifiers might exist; an internal and external. The internal one is typically based on vendor systems for process tracking. The vendor tracking number is unique for that vendor. The external one leverages a publicly available identifier. Common Vulnerabilities and Exposures (CVE) is an example of this method. Once the unique identifier is assigned, it shall be attached to all future correspondence. This can help cut down on many problems in subsequent contact, cross-vendor disclosure, etc.

It is important to note that a internal identifier does not replace a CVE identifier and it can be assigned prior to a CVE ID.

While every care is taken that CVE identifier is unique a situation may occur where an CVE candidate is split into a multiple CVE entries during the subsequent review. This is a rare situation but it can occur.

CVE identifiers, by itself, reveal a certain amount of information and they should be treated as any other sensitive information and not transmitted in cleartext.

f. Sanction against legal action

Vendors should declare that they will not take any legal actions against a finder who follows responsible vulnerability disclosure according to the vendor's published vulnerability handling policy.

g. Vendor credit for finder

Vendor should recognize the contributions of the finder(s) who helped in the discovery or resolution to the vulnerability discovered.

8 Receipt of Vulnerability Information

8.1 General

This clause presents a guideline for vendors to receive information on potential vulnerability from either a finder or a coordinator.

8.2 Acknowledgement of receipt from finder

The vendor once notified of the issue from a finder should issue a receipt to the finder, indicating only a receipt of the notification. In the case, where a finder reports a vulnerability that has already been discovered. The vendor should communicate to the finder this is a duplicate issue. This acknowledgement should respond with a period as specified by the vendor in the vulnerability disclosure policy. This receipt might consist of an e-mail or another electronic means of notification acceptable by both parties.

In some instances a vendor can leverage a case or on-line helpdesk function. This site should be operated by the vendor and should provide the details of the investigation to finder. It is not required that internal process of the vendor be revealed but that they are actively investigating the issue.

8.2.1 Anticipated Response Times and Actions

The vendor should respond to a vulnerability report as soon as possible and as specified in the vendor's vulnerability disclosure policy. However, it is recommended that an acknowledgement of receipt of a vulnerability report be provided to a finder within 7 calendar days of receipt.

8.3 Initial Investigation of Vulnerability

Vendors should inspect the reported potential vulnerability information and decide whether it should be handled as vulnerability. If they decide so, they open a case. The vendor should inform the finder or coordinator of it with rational reasons when they decide not to handle the case as vulnerability.

8.4 Confirmation of Vulnerability

Vendors should check all bug reports, and initiate vulnerability handling if they find vulnerability in them

8.5 Prioritization

Vendors should prioritize the vulnerability for handling appropriately based on information gathered so far. The following list includes items which may be considered to decide the prioritization:

a) Finder's agenda to publicize the vulnerability

A finder may have a plan to describe the vulnerability in their research paper and to present it in some technical conferences. If it is the case, it is favorable for the vendor to disclose it immediately after or earlier than the finder's disclosure. The vendor may request the finder to reconsider his publication agenda, when it is estimated to take longer time to develop its resolution.

b) Population with the knowledge about the vulnerability

Before a vulnerability is reported to the vendor, it possibly has already been disclosed to the public through a blog or a mailing list which has many subscribers. If so, the vendor should keep aware of activities of bad guys trying to find a way to exploit it.

c) Nature of possible attacks

Cost for attack and probability of its success vary depending on the vulnerability to be exploited by the attack. The vulnerability which permits low cost attack with high success probability should be addressed rapidly.

d) Existence and maturity of exploit codes and attack tools

When exploit codes for the vulnerability are available and they work reliably, attack tools based on them are expected to appear before long, which impose security risks on users of the product. In such a case the vendor may have to issue advisories on the vulnerability with only workarounds, even if complete resolution is not available.

e) Nature of potential damage caused by attack

The nature of product and potential damages affect the level of severity of users who are attacked by exploiting the vulnerability. For example, a vulnerability of products used in social critical infrastructures and a vulnerability which may cause a breach of personal data confidentiality need to be addressed as soon as possible.

f) Evidence of attacks (or Incident activity) Evidence of attacks (incidents) that exploit the vulnerability indicate an increased threat against users. Depending on the quality and quantity of incident activity information, the vendor may raise the priority of handling the vulnerability, which may include issuing advisories with only workarounds, even if complete resolution is not available.

8.6 Communication for Reproduction

Vendors may possibly fail to reproduce the vulnerability in their test environment based on the information initially reported by the finder. In such a case, the vendor should ask if the finder can produce further evidence that the issue is a security vulnerability. Vendors should ask the finder about their environment using a standard vulnerability reporting form such as ones shown in Annex B.3.

8.7 Relationship Management with a Finder and/or Coordinator

It is very important for vendors to maintain a good relationship of mutual trust with a finder or a coordinator, especially in the case that it takes long time to finish to handle the vulnerability. Vendors should keep track of each vulnerability case status so that they can provide a timely reply to inquiries from the finder or the coordinator. Vendors should inform them about major case status changes, as this may impact finder or coordinator timelines.

8.8 Communications Channels

Vendors who adopt a policy of vulnerability disclosure will typically offer at web site or page that will used provide information to discoverers, users, and others their accepted methods of possible vulnerable information.

This includes contact information that might include one or more of the following:

- E-mail address
- Phone number
- Name(s) of Individuals to contact
- Secure communication (pub keys and/or fingerprint)

It should clearly state that the information of the said issue information has been received and is being investigated. If situations where further information is required by the vendor the finder should be willing to provide this information upon request. Plain-text e-mail acknowledgement shall minimize exposure of vulnerability details. For example, the message should not list product names. When exchanging sensitive information e-mail messages with details shall be protected by mutually agreed encryption mechanisms such as PGP or OpenPGP. It is recommended that a vendor setup encryption capabilities prior to communication with finders.

Examples of e-mail alias that could be deployed include the following:

- security-alert@example.com
- security@example.com
- secure@example.com

8.9 Contact Window

Vendors should be clarify a window where information of potential vulnerability is received for each their product throughout its lifecycle. A single window for all the products is preferable.

8.10 Support from Co-ordinators

Coordinator can play multiple roles in vulnerability management process:

- Act as trusted introducer between involved parties
- Coordinate advisory public release date
- Enabling communication between involved parties (vendors and finders)
- Provide environment where experts from different organizations can work jointly on addressing the vulnerability

Vendors and finders are encouraged to establish relationship with a coordinator (or more than one coordinator) before start working on a vulnerability. Which coordinator they choose to establish a relationship would depend on various factors as geographical proximity, language and acceptable operation model.

9. Disseminating of Advisory

9.1 General

This clause discusses the advisory aspect of the vulnerability lifecycle and considerations when providing mediation details.

9.2 Disseminating (*or* Sharing) of Vulnerability Information

Editors Note: The editor requests that NB's provide content for this section.

9.2.1 Issues that Affect Multiple Vendors

Some vulnerabilities affect common protocols, software libraries, or otherwise impact multiple vendors. For vulnerabilities that are suspected to affect multiple vendors, vendors should consider notifying a coordinator to help handle vulnerability notification and resolution.

When considering aspects of a multi-vendor vulnerability. The following should be considered:

- Readiness for customer support staff of call centers and sales divisions etc.
- Finder's agenda for publication

- Prevalence of activities exploiting the vulnerability

9.3 Prior to Advisory Release

Vendor should set up a way to release vulnerability information to affected parties. This may commonly include public disclosure, and may also involve private customer notifications. Vendor should create a mailing-list that interested parties can subscribe to. This would include adding the necessary links on vendor web site and posted policy. In order to help advisory consumers with assessing relative impact of different vulnerabilities, vendor should consider using a common vulnerability scoring system (CVSS).

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. It is recommended for Vendors to use a common vulnerability numbering system.

9.4 Dissemination Formatting

Any party producing and distributing vulnerability information as an advisory or any other format should consider the needs of the intended audience both in terms of content and format. Consumers of vulnerability information need to decide if and to what extent they are affected and how best to respond to a vulnerability. An advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references.

Advisory producers shall consider both human and machine-readable formats. Examples of advisories and formats are provided in Annex B.4 –Advisory Samples.

9.5 Public Advisory Release Considerations

If a vendor intends to release an advisory to the public, the following are common considerations for such public release. As all companies and vendors have different web design strategies this clause identifies some considerations when posting advisory information on a web site.

- Clearly identify security information and its location on vendor's website.
- Put the first publication date and the last updated date in the advisory. Consider using the ISO 8601 date format.

Public disclosure and/or private customer notification are chosen considering the following aspects of conditions:

- Shipping and user support scheme for the product.
- Availability of communication channels with which a vendor can rapidly and securely notify all the users of the product without omission.
- A period of estimated time which it takes to finish installing the resolution at each user site.
- Prevalence of activities exploiting the vulnerability.

Annex A – Details to Handling Vulnerability/Advisory Information
(informative)

A.1 Receiving Vulnerability Information

In order to help the vendor in the Verification Phase the vendor can request that the finder provide the following information. The vendor may offer an web site or other electronic means to submit this information. Information useful could include the following:

Product Name
- Product Name
- Operating System
- Version Number using the vendor nomenclature if possible
- Technical Description
- Sample Code
- Finder's Contact Information
- Other Parties Involved
- Disclosure Plan(s)
- Threat/Risk Assessment
- Software Configuration
- Hardware Model
- Hardware Revision Number
- Relevant information about connected devices if vulnerability arises during -interaction
- For online services vulnerabilities, time and date of discovery
- For online services vulnerabilities, URL
- For online service vulnerabilities, browser information including type and version
- For online service vulnerabilities, input required to reproduce the vulnerability

A.2 Vulnerability Disclosure Format

When the vendor is making the information public about their advisory they should consider how the data will provide benefit to comprehend the threat of the vulnerability. The following clauses illustrate information that would be included in a standard vulnerability disclosure. Vendors should provide sufficient information for users to make accurate risk assessments and respond appropriately. Vendors should consistently follow their internal vulnerability handling policy regarding the level of information disclosure.

For vulnerabilities that affect multiple vendors, a neutral third-party coordinator may be engaged. Coordinators should act neutrally and treat all vendors fairly. Coordinators are largely responsible for managing communications among all stakeholders, including multiple vendors and finders.

Overview
Provide summary on the vulnerability first so that the users could understand the essential points quickly.

Vulnerable Software
If possible, provide a descriptive list of affected products and versions. This might also include an explanation 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 cases it may lead to interpreting the incorrect vulnerability and potentially result in a system compromise. It is therefore imperative that a both a

unique numbering and naming convention be used. 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 own might or might not have their own numbering and naming convention. 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
    a. Common Vulnerabilities and Exposures (CVE) Identifiers and dictionary for security vulnerabilities related to software flaws
    b. Common Configuration Enumeration (CCE) Identifiers and dictionary for system configuration issues related to security.
    c. Common Platform Enumeration (CPE). Identifiers and dictionary for platform/product naming
b. Scoring Systems
    a. Common Vulnerability Scoring System (CVSS)

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

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

Threats
Provide information about known threats that relate to the vulnerability, for example the existence of exploit or proof-of-concept code, discussion or evidence of incident activity.

Impact

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 may be the exposure of cookies or other authentication credentials).

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

Workarounds
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, provide the links as reference.

Credit
Some software vendors put contributor for discovering and reporting

Revision History
Clarify the date on which the vulnerability and what was updated.

Contact Information
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 indentified to the end user.

Annex B – Sample Policies, Forms, and Advisories
(informative)

B.1 Sample Vulnerability Disclosure Policy

The following sample can be uses as is or used to build upon. It can be applied to both a software and services based vendor. The policies and statements below does not reflect legal guidance and it is recommended that any company that posts a policy seek legal council 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 <companies 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 7 days.

Receiving Security Information from <Company Name>

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

1. <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've identified a practical workaround or fix for the particular security vulnerability though there may 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 may take alternative actions in connection with issuing security notices. <Company name> may 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 may consider significant or that notices will be issued on any specific timetable.

2. Security-related information may 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.

3. <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 Identifying and Managing Risk in Systems

To help reduce vulnerabilities from software and hardware it best to start off with a secure development process. The following two IS can be used to learn more about mitigating risk to address these concerns:

a. ISO/IEC 16085:2006 Systems and Software Engineering – Life Cycle Processes and Risk Management – ISO/IEC 16085:2006 defines a process for the management of risk in the life cycle. It can be added to the existing set of system and software life cycle processes defined by ISO/IEC 15288 and ISO/IEC 12207, or it can be used independently.

   ISO/IEC 16085:2006 can be applied equally to systems and software.

   Risk management is a key discipline for making effective decisions and communicating the results within organizations. The purpose of risk management is to identify potential managerial and technical problems before they occur so that actions can be taken that reduce or eliminate the probability and/or impact of these problems should they occur. It is a critical tool for continuously determining the feasibility of project plans, for improving the search for and identification of potential problems that can affect life cycle activities and the quality and performance of products, and for improving the active management of projects.

b. ISO/IEC 27005:2008 Information Technology – Security Techniques – Information Security Risk Management – ISO/IEC 27005:2008 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2008. ISO/IEC 27005:2008 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

c. CERT Resiliency Management Model http://www.cert.org/resiliency/rmm.html
   Editors Note: The editor requests that NBs provide more content for this section

d. Building Security in Maturity Model http://www.bsi-mm.com/
   Editors Note: The editor requests that NBs provide more content for this section

B.3 Vulnerability Reporting Form Examples

B3.1 CERT/CC Vulnerability Reporting Form

Vulnerability Reporting Form

We accept reports of security vulnerabilities and serve as a co-ordinating 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
May 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 may 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 may 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.

B3.2 IPA and JPCERT Vulnerability Reporting Form

0. 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 web site.

(If not the case, IPA can't receive and handle the vulnerability report.)

1. 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 two:

   1. The reporter agrees that IPA may send the reporter's contact information to JPCERT/CC and the product vendor.
   2. 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.

3. Reference to the reporter in acknowledgement of advisories

    1. In advisories by JPCERT/CC choose one from the following two:
        a. The reporter's name and/or affiliation may be included.
        b. The reporter's name and/or affiliation must not appear.
    2. In advisories by product vendors choose one from the following two:
        a. The reporter's and/or affiliation name may be included.
        b. The reporter's and/or affiliation name must not appear.

    If the reporter's name may 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:

2. Vulnerability related information

1. Source of the information choose one from the following three:
    a. Reporter itself
    b. Reporter's acquaintance
    c. BBS, blog and so on (URL:)
2. Product in which the vulnerability is found
    a. Product name:
    b. Software version:
    c. Patch and fix:
    d. Language version:
    e. Deviation from standard configuration:
    f. Product vendor's name:
    g. Product vendor's URL:

Information about a miner 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:
    a. Always
    b. Often
    c. 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)

3. 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 is has been distributed in overseas countries or not.
    5. Other( )

4. 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.

5. 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.

6. Other items which should be reported

B.4 Advisory Samples

B.4.3 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.mspx

B.5 National Infrastructure Advisory Council Vulnerability Framework

NIAC was a consortium consisting of United States based companies that developed a framework to then President George W. Bush. All though specifically written with a US focus there are many aspects that play a role globally such as identifying, reporting, scoring, remediation, and resolution. Specific to this International Standard which focuses on reporting, remediation and resolution. The NIAC Framework was written for product vulnerabilities in particular, and does not cover cases of online services vulnerabilities."

The identified vulnerability resolution lifecycle currently aligns to those contained within this International Standard.

B.6 Coordinators Recognized Globally

The following, non-exhaustive, list of globally recognized coordinators is correct at the time this IS was last updated. Since then new coordinators may become active or an existing coordinators may scale back their capabilities.

Australian Computer Emergency Response Team (AuCERT) - www.auscert.org.au

CERT/CC (Software Engineering Institute (SEI) CERT Program of Carnegie Mellon University) – 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/

Bibliography

[1] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[2] ISO/IEC 15408-1, Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework

[3] ISO/IEC 19770-1:2006, Information technology – Software asset management – Part 1: Processes

[4] ISO/IEC TR 19791, Information technology – Security techniques – Security assessment of operational systems

[5] ISO/IEC 20000-1, Information technology – Service management – Part 1: Service management system requirements

[6] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements

[7] ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management

[8] ISO/IEC 27035 (to be published), Information technology – Security techniques – Information security incident management