



ISO/IEC JTC 1/SC 27 **N7901**

ISO/IEC JTC 1/SC 27/WG 3 **N1001**

REPLACES: N7267

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: text for working draft

TITLE: Text for ISO/IEC 3rd WD 29147 – Information technology – Security techniques – Responsible vulnerability disclosure

SOURCE: Project Editor (F. Khan)

DATE : 2009-06-25

PROJECT: 29147

STATUS: In accordance with resolution 2 (contained in SC 27 N7777) of the 21st SC 27 Plenary meeting held in Beijing (China) 11th - 12th May 2009, this document is being circulated to National Bodies and liaison organizations for study and comment.

The National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the hereby attached document directly to the SC 27 Secretariat as soon as possible but no later than **2009-10-06**.

PLEASE NOTE: For comments please use THE SC 27 TEMPLATE separately attached to this document.

ACTION: COM

DUE DATE: 2009-10-06

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 30

Reference number of working document: **ISO/IEC JTC 1/SC 27 N 7901**

Date: 2009-07-06

Reference number of document: **ISO/IEC 3rd WD 29147**

Committee identification: **ISO/IEC JTC 1/SC 27/WG 3**

Secretariat: **DIN**

Information technology – Security techniques -- Responsible 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.

Document type: **International standard**

Document subtype: **if applicable**

Document stage: **(20) Preparation**

Document language: **E**

X:\TA3\TG3-3\NA043\NA043_Sekretariat\JTC1_SC27\03_Projekte\PROJECT_admin\29147_Responsible_Vulnerability_Disclosure_Mar2008\02_03_3rdWD_29147_20090625\SC27N7901_3rdWD_29147_20090625\SC27N7901_3rdWD_29147_RVD_20090625_with_changes.doc Basic template BASICEN3 2002-06-01

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

*Secretariat ISO/IEC JTC 1/SC27
DIN German Institute for Standardization
DE – 10772 Berlin
Germany*

*Tel: +49 30 2601 2652
Fax: +49 30 2601 1723
E-mail: krystyna.passia@din.de
Web: www.jtc1sc27.din.de/en
<http://isotc.iso.org/isotcportal/index.html> (SC 27 documents)*

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Symbols (and abbreviated terms).....	3
5 Responsible Vulnerability Disclosure	3
6 Life Cycle of a Vulnerability	3
6.1 Vulnerability Handling Policy	5
7 Vulnerability Handling Policy Considerations	5
7.1 Secure Receiving Model (SRM).....	5
7.2 Issues that Affect Multiple Vendors	5
7.3 Acknowledgement of receipt from finder	6
7.4 Obtaining a CVE Number.....	6
7.5 Communications Channels	6
7.6 Anticipated Response Times and Actions	6
7.7 Conflict Arbitration between a Vendor and Finder	7
8 Disseminating of Vulnerability Information	7
8.1 Dissemination Formatting	7
8.2 Special Considerations.....	7
8.3 Web Site Considerations	7
A.1 Receiving Vulnerability Information	9
A.2 Advisory Considerations.....	13
A.3 Advisory Examples	14
A.4 National Infrastructure Advisory Council Vulnerability Framework	18
A.5 CERT and Coordinators Globally	19
B.1 Sample Vulnerability Disclosure Policy	21
B.2 Identifying and Managing Risk in Systems	22
Bibliography.....	24

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 should 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

Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a vulnerability. Users, businesses, and governments have increased their reliance on networks, applications, and the Internet for core operations and critical infrastructure. Vulnerabilities in technology vital to operations represent an increased risk. The key stakeholders in this process; finders, vendor, sub-component owner and coordinators have the same objective: reduce or eliminate vulnerabilities to ensure continued delivery of critical services and timely secure flow of information.

Responsible Disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce users' risks associated with the vulnerability.

This International Standard provides a guideline for vendors on receiving information about potential vulnerabilities in a uniform way. This document also provides guidance for vendors to distribute vulnerability resolution information.

Information technology – Security techniques -- Responsible vulnerability disclosure

1 Scope

This International Standard gives guidelines for the vendor to receive information about a potential vulnerability and to disseminate resolution information to be used by all interested parties.

The vendor may include the following; software vendor, hardware vendor, application service provider and on-line/web application provider. The vendor may act as a Finder or in some instances as both when using a 3rd party software subcomponent.

The vendors identified in this International Standard are any person(s) and/or organization(s) responsible to investigate a potential vulnerability in a component created, developed or maintained by that person(s) and/or organization.

This IS aims to ensure that vendors have the capability for receiving information about a potential vulnerability and the capability for disseminating vulnerability resolution information to all interested parties.

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.

<Add links as comments are provided>

3 Terms and definitions

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

3.1

finder

person or organization who identifies the vulnerability

3.2

vendor

person, organization, or company that developed the software, application, web service, or is responsible for maintaining it

3.3

coordinator

An optional participant that can serve as a proxy between the Vendor and Finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process

3.4

vulnerability

a weakness in a system which, if exploited, allows the exploiter to violate the security policy for the that system

NOTE 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.

3.5
software
<Check with SC7>

3.6
application
<Check with SC7>

3.7
update
patch, fix, upgrade, or configuration change to address a vulnerability

NOTE A software 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 and upgrade.

3.8
vendor
person, organization, or company that developed the software, application, web service, or is responsible for maintaining it

3.9
responsible vulnerability disclosure
private advance disclosure of a vulnerability to a Vendor or Coordinator, where Vendor is allowed time to produce a fix prior to public disclosure

3.10
vulnerability
a weakness in a system which, if exploited, allows the exploiter to violate the security policy for that system

NOTE 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.

3.11
security incident
evidence of attacks that attempt to exploit a vulnerability, whether successful or not

3.12
vulnerability information service
an organization that acts as an aggregator or distributor for vulnerability information

NOTE Finders and Vendors can provide information to these services or add references to them when publishing vulnerability information.

3.13
advisory
an advisory may be published by a Vendor, Finder, or Coordinator

NOTE An Advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references.

4 Symbols (and abbreviated terms)

< Build as comments are provided >

5 Responsible Vulnerability Disclosure

Responsible Disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce user's risks associated with the vulnerability.

The benefits of responsible disclosure and vulnerability handling include the following:

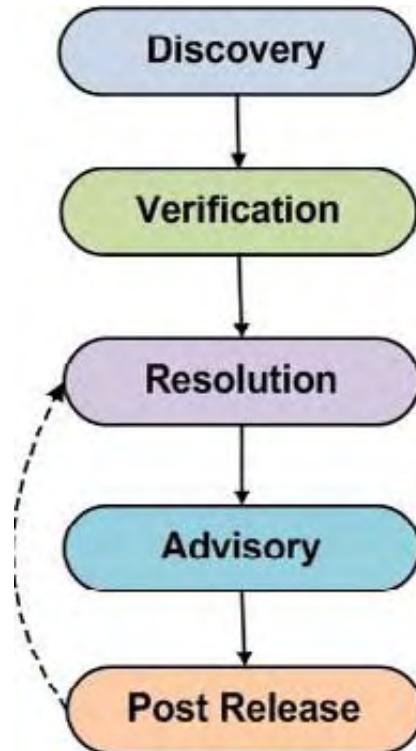
- It can minimize the risk posed by security vulnerabilities, by enabling them to be identified, investigated, and resolved in a way that produces a timely – quality remedy that will have high uptake among the affected systems
- It can also contribute to improving the engineering quality of software products, by supporting the academic and research communities' ongoing efforts to identify common security vulnerabilities, the conditions under which they occur, and methods to avoid them

This process will begin by creating a vulnerability disclosure policy and making it publically available. This will ensure that all Finders will know how to contact your organization and the exact process of working with your organization for addressing potential vulnerability issues.

This IS first outlines the phases of vulnerability processing then goes on to provide some guidance for creating a policy. This concludes with issuance of advisory and insight to potential issues that will surround this process.

6 Life Cycle of a Vulnerability

Regardless of the nature of a vulnerability, each one being unique, some elements of reporting and identifying are identical. The following lifecycle aligns these common phases.



1. Discovery Phase

- a. Discovery: A finder discovers a potential security vulnerability
- b. Notification: The finder notifies the vendor(s) of the potential vulnerability
- c. Acknowledgement: Vendors acknowledge receipt of the report,

2. Verification Phase

- a. Initial Investigation: The vendor attempts to reproduce the vulnerability
- b. 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.
- c. Further Investigation: Attempt to find other instances of the same type of vulnerability
- d. Triage: Determine severity of the vulnerability

3. Resolution Phase

- a. Action Point: Vendor determines how they will deal with the vulnerability
- b. Produce Update: patch, fix, upgrade, or configuration change to address a vulnerability
- c. Test Update: perform a reasonable amount of test cases to ensure the vulnerability issue has been addressed

4. Advisory Phase

- a. Update Release: Once the vendor is satisfied that the patch is effective and not harmful to most customer software environments, it notifies customers and the general public via an advisory.

5. Post Release Phase

- a. Case Closure: 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.
- b. 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 issue. They can be aligned to two primary functions receiving and dissemination. The receiving aspect deals with obtaining the details of the possible vulnerability. The dissemination aspect focuses on getting that information to all

interested parties. The remainder of this document focuses on these two primary aspects including some initial preparatory details for organizations that lack process maturity.

6.1 Vulnerability Handling Policy

A policy should state the intentions of the vendor as it relates to vulnerability reporting. This might include contact information, timelines, communications channels, etc. It can be as open as the vendor is willing to operate. Several examples are listed in Appendix B1 Sample Vulnerability Reporting Policy.

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

1. How the organization 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 level and should write this section appropriately to match their capabilities.

2. Expected turn around times for responses and action

Vendors should explain/set expectations for communication, including initial acknowledgement of receipt of report and status updates.

3. 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.

An sample policy is contained in Appendix B1: Sample Vulnerability Disclosure Policy.

7 Vulnerability Handling Policy Considerations

This section discusses in detail some considerations when creating a policy. As each Vendor who creates software and hardware will have different requirements and resources available for dealing with security vulnerability information; understanding some of these topics in detail will help to provide guidance when they arise.

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 provide the details of communications methods and available encrypted mail certificates in the vulnerability disclosure policy.

7.2 Issues that Affect Multiple Vendors

Some vulnerabilities affect common protocols, software libraries, or otherwise impact multiple vendors. To the extent possible, finders and vendors should notify all affected vendors, either directly or through coordinators.

In the case, finders and vendors may notify all the affected vendors through coordinators. They may also directly do it if they can do comprehensively.

7.3 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, and assigning an internal tracking number. This acknowledgement should respond with a period as specified by the vendor in the vulnerability disclosure policy. However, it is recommended that a response be provided within 14 days of receipt. This receipt might consist of an e-mail or another electronic means of notification acceptable by both parties.

If e-mail is agreed upon, this e-mail should be sourced using and address from the receiving parties official mail domain registration. 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 should minimize exposure of vulnerability details. For example, the message should not list product names. Pre-disclosure e-mail messages with details should be protected by mutually agreed encryption mechanisms such as PGP.

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

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

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.

7.4 Obtaining a CVE Number

At the time of receiving vulnerability information neither the Finder nor Vendor will be required to assign or obtain a CVE number. Larger vendors are typically provided a block of CVE numbers that can be used when the data received is recognized as a vulnerability and the advisory is made public. Otherwise smaller organizations can contact CVE directly to obtain a number.

7.5 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. An individual regardless of organization public or private will be referred to as a “finder”.

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)

7.6 Anticipated Response Times and Actions

Vendors should acknowledge receipt of the vulnerability report from the Finder within 14 days.

7.7 Conflict Arbitration between a Vendor and Finder

In some situations a dispute will arise between a vendor and finder. It hoped that both parties would attempt to find a solution with increased communications. However, in some instances this might not be achievable. In these situations it is recommended that a coordinator be used as an intermediary. They would function on behalf of the vendor and interface to both the finder and vender. These are internationally recognized organizations typically and nations will have at least one. If a nation they can leverage the services of a larger coordinator, a list of some of these is contained in Appendix A4: CERT and Coordinators Globally.

Conflict situations might include the following:

- Insufficient information provided to vendor to assess the claim
- Acknowledgement of vulnerability information sent not being received, including follow-up requests for the acknowledgement
-

The coordinator should be vendor neutral and willing to work with all parties involved.

8 Disseminating of Vulnerability Information

Vendors should set up a way to release advisories to the public. This can be via a web page, a mailing list, or another delivery mechanism of their choosing. 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, such as CVE (Common Vulnerabilities and Exposures), to identify specific vulnerabilities described in advisories. If multiple Vendors are releasing advisories on the same vulnerability, each Vendor should use the same common identifier, such as CVE number.

8.1 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 should consider both human and machine-readable formats. Examples of Advisories and formats are provided in Appendix X.

8.2 Special Considerations

When a vendor is producing an advisory there might be situations when they might want to deviate from the normal processing. This section provides guidance to these situations and what can be done.

Finder releases vulnerability information before agreed date

Vendor (has and internal leak of information)

Vulnerability is wide spread and requires a coordinated effort

8.3 Web Site Considerations

As all companies and organizations have different web design strategies this section identifies some considerations when posting advisory information on a web site.

- If the web site has a deep hierarchy or the layout is complicated, it is difficult for the users to get to vulnerability information. Make sure that the users do not have to go through the layers of web pages to view vulnerability information

- For the link to each vulnerability information, use the title of each vulnerability as its hyperlink text.
- Put the last updated date such as 1.3.10 (Revision History).

Annex A (normative)

A.1 Receiving Vulnerability Information

In order to better process the steps in the Verification Phase it is requested to provide the following information to a vendor. The vendor may offer an web site or other electronic means to submit this information. Information useful could include the following:

- Product Name
- 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

The following are two examples for submitting this.

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

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.

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 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:
 - 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 it 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

A.2 Advisory Considerations

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 sections illustrate information that would be included in a standard vulnerability disclosure. Vendors can determine the level of information to provide based on severity of the vulnerability identified.

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:

Xxxxxx: Name

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

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 developers 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 patch has caused some trouble.

A.3 Advisory Examples

Example from US CERT

Vulnerability Note VU#905281

Adobe Reader and Acrobat JBIG2 buffer overflow vulnerability

Overview

Adobe Reader and Acrobat contain a buffer overflow vulnerability that may allow an attacker to execute arbitrary code.

I. Description

Adobe Acrobat Reader is software designed to view Portable Document Format (PDF) files. Adobe also distributes the Adobe Acrobat Plug-In to allow users to view PDF files inside of a web browser. Adobe Reader and Acrobat contain a buffer overflow vulnerability in the handling of JBIG2 streams.

Exploit code for this vulnerability is publicly available.

II. Impact

By convincing a user to open a malicious PDF file, an attacker may be able to execute code or cause a vulnerable PDF viewer to crash. The PDF could be emailed as an attachment or hosted on a website.

III. Solution

Apply an update

This issue is addressed in Adobe Reader and Acrobat versions 9.1, 8.1.4, and 7.1.1. More details are available in Adobe Security Bulletin APSB09-03 and APSB09-04.

Disable JavaScript in Adobe Reader and Acrobat

Disabling JavaScript may prevent this vulnerability from being exploited. Acrobat JavaScript can be disabled in the General preferences dialog (Edit -> Preferences -> JavaScript and un-check Enable Acrobat JavaScript). Note that this will not block the vulnerability. Adobe products still may crash when parsing specially crafted PDF documents. Disabling JavaScript will mitigate a common method used to achieve code execution with this vulnerability. Also note that when JavaScript is disabled in Adobe Reader, the software will

prompt the user to enable JavaScript when it opens a document that uses the feature. So although JavaScript is a single click away, setting this preference can help mitigate exploits that use JavaScript. Some have reported that they have successfully achieved code execution without the use of JavaScript.

Some vendors ship JavaScript support in a separate package. Removing this package may remove JavaScript support in the Adobe PDF reader.

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 behavior can be reverted to the safer option of prompting 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 displaying of PDF documents in the web browser

Preventing PDF documents from opening inside a web browser may mitigate this vulnerability. If this workaround is applied to updated versions of the Adobe reader, it may mitigate future vulnerabilities.

To prevent PDF documents from automatically being opened in a web browser:

1. Open Adobe Acrobat Reader.
2. Open the Edit menu.
3. Choose the preferences option.
4. Choose the Internet section.
5. Un-check the "Display PDF in browser" check box.

Disable Adobe Acrobat Windows Shell integration

Adobe Acrobat and Reader integrates itself with the Windows shell. The file pdfshell.dll is used to configure Windows Explorer to launch Adobe components to render, preview, and obtain details from a PDF document, all without actually opening the PDF document itself. Windows Shell integration for Adobe Acrobat and Reader can be disabled by unregistering the pdfshell.dll by running the following command:

```
regsvr32 /u "%CommonProgramFiles%\Adobe\Acrobat\ActiveX\pdfshell.dll"
```

Disable the Adobe Acrobat Indexing Service filter

Adobe Reader and Adobe Acrobat install an Indexing Service filter that is used to parse PDF files. These filters are provided by AcroRdIF.dll and AcroIF.dll, respectively. When an application that uses the Adobe IFilters indexes a malicious PDF document, the vulnerability may be triggered. This attack vector can be mitigated by unregistering the Adobe IFilter files.

Adobe Acrobat users should locate the Acrobat directory and run: regsvr32 /u AcroIF.dll

Adobe Reader users should locate the Adobe Reader directory and run: regsvr32 /u AcroRdIF.dll

Note: After disabling the Windows shell integration or the Indexing Service filter by unregistering the appropriate DLL, the Windows Installer MSI resiliency feature may trigger a "repair" of those features when an advertised shortcut for Adobe Reader is clicked. To prevent this from occurring, delete the Adobe Reader icon from the Windows start menu and then re-create a normal, non-advertised shortcut. More details are available in the CERT/CC Vulnerability Analysis Blog.

Do not access PDF documents from untrusted sources

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

Vendor Status Date Notified Date Updated
Adobe Vulnerable 2009-02-19 2009-03-11
References

<http://www.us-cert.gov/cas/tips/ST04-010.html>
http://www.cert.org/tech_tips/securing_browser/
http://www.cert.org/blogs/vuls/2009/03/windows_installer_application.html
<http://www.adobe.com/support/security/advisories/apsa09-01.html>
<http://www.adobe.com/support/security/bulletins/apsb09-03.html>
<http://www.avertlabs.com/research/blog/index.php/2009/02/19/new-backdoor-attacks-using-pdf-documents/>
<http://jbig2.com/>
<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20090219>
<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20090221>
<http://vrt-sourcefire.blogspot.com/2009/02/homebrew-patch-for-adobe-acroreader-9.html>
<http://secunia.com/blog/44/>
<http://www.milw0rm.com/exploits/8090>
Credit

Thanks to Adobe for information that was used in this report.

This document was written by Will Dormann and Ryan Giobbi.

Other Information

Date Public: 2009-02-19
Date First Published: 2009-02-20
Date Last Updated: 2009-03-18
CERT Advisory:
CVE-ID(s): CVE-2009-0658
NVD-ID(s): CVE-2009-0658
US-CERT Technical Alerts:
Metric: 32.91
Document Revision: 95

If you have feedback, comments, or additional information about this vulnerability, please send us email.

Example from Cisco

Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, March 25, 2009

Document ID: 109732

Advisory ID: cisco-sa-20090325-bundle

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml>

Revision 1.2

Last Updated 2009 June 1 1800 UTC (GMT)

For Public Release 2009 March 25 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

- Summary
- Software Versions and Fixes
- Obtaining Fixed Software
- Status of this Notice: FINAL
- Distribution
- Revision History
- Cisco Security Procedures

Summary

The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory, and each security advisory also lists recommended releases that correct the vulnerabilities in the other seven advisories. The table in this document lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

Individual publication links are listed below:

- * Cisco IOS cTCP Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>

- * Cisco IOS Software Multiple Features IP Sockets Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- * Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>

- * Cisco IOS Software Secure Copy Privilege Escalation Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>

- * Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml>

- * Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>

- * Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>

- * Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

View the full advisory located at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml>

Example of Microsoft Security Bulletin

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 subsection, Affected and Non-Affected Software, in this section.

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>

Example of CVE

CVE-2009-2031

smbfs in Sun OpenSolaris snv_84 through snv_110, when default mount permissions are used, allows local users to read arbitrary files, and list arbitrary directories, on CIFS volumes.

View the full report at <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2031>

Example of CVSS

Example of CPE

A.4 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 IS which focuses on reporting, remediation and resolution.

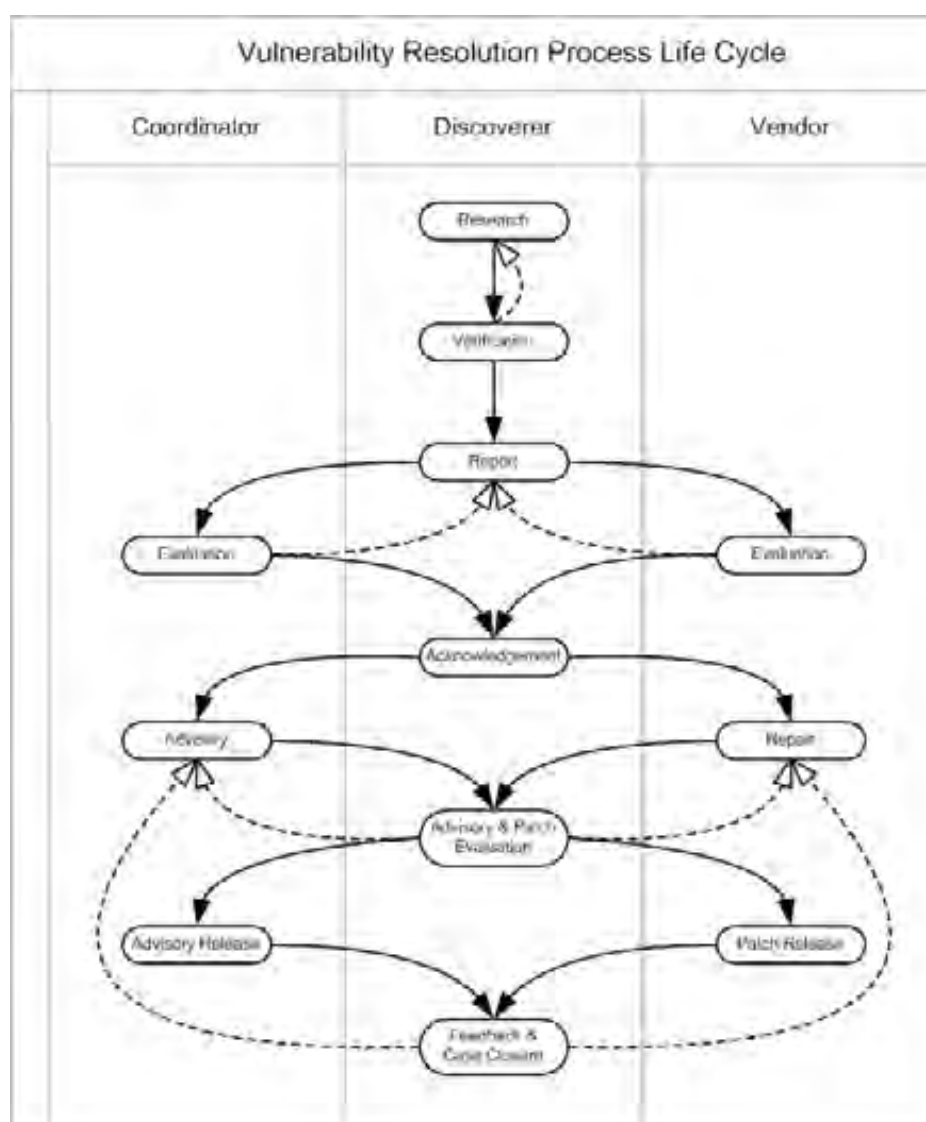
The following seven recommendations are made to the President to direct appropriate Departments and Agencies involved in any aspect of managing software vulnerabilities.

- Support development of a common vulnerability management architecture, including common terms and universally compatible procedures to be employed in the public and private sectors for identifying, reporting, scoring, remediating, and resolving vulnerabilities. This includes standardized E-mail

addresses for reporting and standardized Web site locations and content for sharing information effectively.

- Provide policy and funding to ensure that trusted environments are available to protect vulnerability information and ongoing investigations.
- Promote universal use of multiple compatible encryption methods to ensure the U.S. federal government can participate effectively in the global vulnerability management process.
- Conduct a regulatory framework review. The federal government should review existing federal regulations and practices in order to identify barriers to resolving software vulnerabilities.
- Support robust voluntary information sharing through policy and funding. The federal government should set up or support neutral clearinghouses for vulnerability management, accessible to researchers, the private sector, and federal agencies.
- Support a robust infrastructure for international coordination.
- Promote and fund advanced university and industry security research and education.

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



A.5 CERT and Coordinators Globally

The following list identifies global centres for vulnerability disclosure.

JPCERT - www.jpCERT.or.jp/english/

CERT/CC – www.cert.org

AuCERT - www.auscert.org.au

Annex B (informative)

B.1 Sample Vulnerability Disclosure Policy

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

Security Vulnerability Reporting Policy

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 Incident Response Team

Contact the <company name> Security Incident Response Team (SIRT) by sending email to security-alert@<companyname.com> 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 14 days.

Responding to Customer Incidents

<Company name> plays a supporting role in responding to customer security incidents, offering technical support and expertise. However, final decision-making regarding how incidents are handled remains with the customer and/or end user of the product and/or service.

<Company name> reserves the right to determine the type and degree of assistance it may offer in connection with any incident, and to withdraw from any incident at any time. <Company Name> may give special consideration to security incidents that involve actual or potential threats to persons, property, or the Internet, as well as requests from law enforcement agencies or formal incident response teams.

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 <name of local CERT agency> 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.

Bibliography

- [1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2001
- [2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*
- [3] ISO 10241, *International terminology standards — Preparation and layout*
- [4] ISO 128-30, *Technical drawings — General principles of presentation — Part 30: Basic conventions for views*
- [5] ISO 128-34, *Technical drawings — General principles of presentation — Part 34: Views on mechanical engineering drawings*
- [6] ISO 128-40, *Technical drawings — General principles of presentation — Part 40: Basic conventions for cuts and sections*
- [7] ISO 128-44, *Technical drawings — General principles of presentation — Part 44: Sections on mechanical engineering drawings*
- [8] ISO 31 (all parts), *Quantities and units*
- [9] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*
- [10] ISO 1000, *SI units and recommendations for the use of their multiples and of certain other units*
- [11] ISO 690, *Documentation — Bibliographic references — Content, form and structure*
- [12] ISO 690-2, *Information and documentation — Bibliographic references — Part 2: Electronic documents or parts thereof*
- [13] Guidelines for Security Vulnerability Reporting and Response Process V2.0 by OIS <http://www.oisafety.org/guidelines/secresp.html>
- [14] "Vulnerability Disclosure Framework" by NIAC <http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf>
- [15] "Full Disclosure Policy (RFPolicy) v2.0" by Rain Forest Puppy <http://www.wiretrip.net/rfp/policy.html>
- [16] "Responsible Vulnerability Disclosure Process" by Steve Christey and Chris Wysopal <http://www.wiretrip.net/rfp/txt/ietf-draft.txt>
- [17] CERT/CC Vulnerability Disclosure Policy http://www.cert.org/kb/vul_disclosure.html
- [18] Cisco Security Vulnerability Policy
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
- [19] VULDEF: The Vulnerability Data publication and Exchange Format data model <http://jvnrss.ise.chuo-u.ac.jp/jtg/vuldef/index.en.html>
- [20] CAIF - Common Announcement Interchange Format <http://www.caif.info/>