



ISO/IEC JTC 1/SC 27 **N8126**

ISO/IEC JTC 1/SC 27/WG 3 **N38126**

REPLACES: N7901

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

- DOC TYPE:** text for working draft
- TITLE:** Text for ISO/IEC 4th WD 29147 – Information technology – Security techniques – Responsible vulnerability disclosure
- SOURCE:** Project Editor (F. Khan)
- DATE :** 2010-01-19
- PROJECT:** 29147 (1.27.65)
- STATUS:** In accordance with resolution 5 (contained in SC 27 N8115) of the 39th SC 27/WG 3 Plenary meeting held in Redmond (WA, USA) 2nd – 6th November 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 **2010-03-15**.
- PLEASE NOTE:** For comments please use THE SC 27 TEMPLATE separately attached to this document.
- ACTION:** COM
- DUE DATE:** 2010-03-15
- 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 + 26

Reference number of working document: ISO/IEC JTC 1/SC 27 N **8127**

Date: 2010-01-19

Reference number of document: ISO/IEC 4th **WD 29147**

Committee identification: ISO/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: English

D:\HOD_South_Africa\Eigene Dateien\PROJECT_admin\29147_Responsible_Vulnerability_Disclosure_Mar2008\02_04_4th_WD_29147_20100119\SC27N8126_4thWD_29147_20100119\SC27N8126_4thWD_29147_20100119.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 of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10772 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 1723
E-mail krystyna.passia@din.de
Web <http://www.jtc1sc27.din.de/en> (public web site)
<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	iv
Introduction.....	v
1 Scope.....	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms)	2
5 Responsible Vulnerability Disclosure.....	3
7 Vulnerability Handling Policy	5
8 Receipt of Vulnerability Information	5
8.2 Secure Receiving Model (SRM).....	6
8.3 Acknowledgement of receipt from finder	6
8.4 Assigning a Unique Identifier to a Vulnerability	6
8.5 Communications Channels	6
9.0 Disseminating of Vulnerability Information	7
9.1 Dissemination Formatting	7
9.2 Issues that Affect Multiple Vendors	7
Annex A – Details to Handling Vulnerability/Advisory Information (informative)	9
A.2 Vulnerability Disclosure Format.....	9
Annex B – Sample Policies, Forms, and Advisories (informative)	12
B.1 Sample Vulnerability Disclosure.....	12
B.2 Identifying and Managing Risk in Systems	13
B.6 National Infrastructure Advisory Council Vulnerability Framework	18
B.7 Coordinators Recognized Globally.....	19
Bibliography.....	20

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.

Introduction

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

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.

Through responsible 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.

As defined by reference 15 in the bibliography, "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.

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

Information technology – Security techniques -- Responsible vulnerability disclosure

1 Scope

This International Standard gives guidelines for vendors to receive information about potential vulnerabilities and to disseminate resolution information.

The vendor can include the following; software vendor, hardware vendor, application service provider and on-line/web application provider.

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

This International Standard 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 stakeholders.

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.

3 Terms and definitions

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

3.1 advisory

a vulnerability advisory may include advice on how to deal with the vulnerability.

NOTE 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."

3.2 coordinator

person or organization that serves as a proxy between the supplier and the finder, assists with technical evaluations, coordinates among multiple vendors, or performs other functions to promote the effectiveness of the vulnerability response process

NOTE Participation of a coordinator is optional

3.3 finder

person or organization who discovers a potential vulnerability

3.4

product

item developed, manufactured or refined for sale

NOTE 1 A service is generally not viewed as a product

NOTE 2 A product is often developed using a systems approach

NOTE 3 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 it uses software

3.5

online services

an organization that provides an information service over the Internet

NOTE 1 The content being hosted can be of a proprietary nature

EXAMPLE Search engines, online backup services and application service providers are considered to be online services

3.6

security incident

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

3.7

update

patch, fix, upgrade, or configuration 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 and upgrade.

3.8

vendor

person, organization, or company that developed the software, hardware or online service, or is responsible for maintaining it.

3.9

vulnerability

weakness of an asset or control that can be exploited by a threat

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.

4 Abbreviated terms)

BBS bulletin board system

CC common criteria

CCE common configuration enumeration

CERT computer emergency response team

CPE common platform enumeration

CVE common vulnerability enumeration
CVSS common vulnerability scoring system
DLL dynamic link library
ID identification
IPA information technology promotion agency
JPCERT Japan computer emergency response team
URL uniform resource locator
PDF portable document format
POC proof of concept
PGP pretty good privacy
SIRT security incident response team
SRM secure receiving model

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.

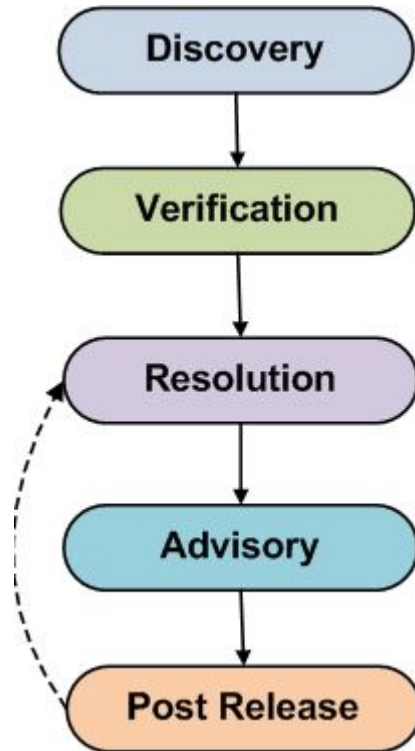
The benefits of responsible disclosure and vulnerability handling include the following:

- It can increase the customer's trust in the vendor and its product through information disclosure, which can minimize the risks of the customer.
- 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 insecure development methods and practices, including insecure design and coding that result in security vulnerabilities, the conditions under which they occur, and methods to avoid them."

Before responsible vulnerability disclosure between a finder and vendor can begin, the vendor first must ensure they have established and made publically available their vulnerability disclosure policy".

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.
- e. Exploit investigation: Attempt to determine whether the vulnerability has been exploited so far and how widespread the exploitation is.

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.
- d. Production system update: for online services vulnerabilities, implement the resolution in the production system.

4. Advisory Phase

- a. Update Release: Once the vendor is satisfied that the update is effective it notifies customers and possibly 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. 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 .

7 Vulnerability Handling Policy

Vendors shall define their responsibilities in the vulnerability handling policy. For an example, see the internet draft on RVD process (<http://tools.ietf.org/draft/draft-christeywysopal-vuln-disclosure/draft-christeywysopal-vuln-disclosure-00.txt>). A policy shall 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 Annex B.1 Sample Vulnerability Reporting Policy.

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

1. How the vendor would like to be contacted

This can be 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. 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.

2. Expected responses

Vendors shall 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.

4. 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".

5, Special Considerations

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.

8 Receipt of Vulnerability Information

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. This clause discusses considerations to be taken into account when creating a policy.

8.1 Simplified Policy

The vulnerability handling policy should avoid complicated steps to avoid discouraging the vulnerability reporting to the vendor.

8.2 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.

8.3 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 shall 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.

It shall 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 shall be willing to provide this information upon request. Plain-text e-mail acknowledgement shall minimize exposure of vulnerability details. For example, the message shall not list product names. Pre-disclosure e-mail messages with details shall 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

In some instances a vendor can leverage a case or on-line helpdesk function. This site shall be operated by the vendor and shall 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.

8.4 Assigning a Unique Identifier to a Vulnerability

A unique identifier, typically a number shall 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. 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. Common Vulnerabilities and Exposures (CVE) identifiers could be used for this purpose."

8.5 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)

8.6 Anticipated Response Times and Actions

The vendor shall 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.

8.7 Role of a Coordinator

In some situations a dispute will arise between a vendor and finder. It is 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 vendor. 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 coordinators is contained in Annex B.7: Coordinators Recognized 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 shall be vendor neutral and willing to work with all parties involved.

9.0 Disseminating of Vulnerability Information

Vendors 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. 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 shall 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.

9.1 Dissemination Formatting

Any party producing and distributing vulnerability information as an Advisory or any other format shall 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 – Sample Advisories.

9.2 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.

9.2 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.

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 shall 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 shall 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 shall 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.

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

B.1 Sample Vulnerability Disclosure

The following sample can be used as is or used to build upon. It can be applied to both a software and services based vendor. 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> Computer Security Incident Response Team (CSIRT)." 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.

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 regional CSIRT 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.

B.3 Vulnerability Reporting Form Examples

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

B.4 Advisory Examples

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.msp>

B.5 Samples of Good and Bad Disclosure

The following are some disclosures that reference either good or bad methodology based on this International Standard.

AppRiver servers as a recent example of excellent disclosure handling:

<http://holisticinfosec.blogspot.com/2009/08/appriver-saas-security-provider-sets.html>

Ameriprise/American Express as a example of disclosure handling gone wrong:

<http://holisticinfosec.blogspot.com/2009/08/appriver-saas-security-provider-sets.html>

<http://holisticinfosec.blogspot.com/2008/12/online-finance-flaw-american-express.html>

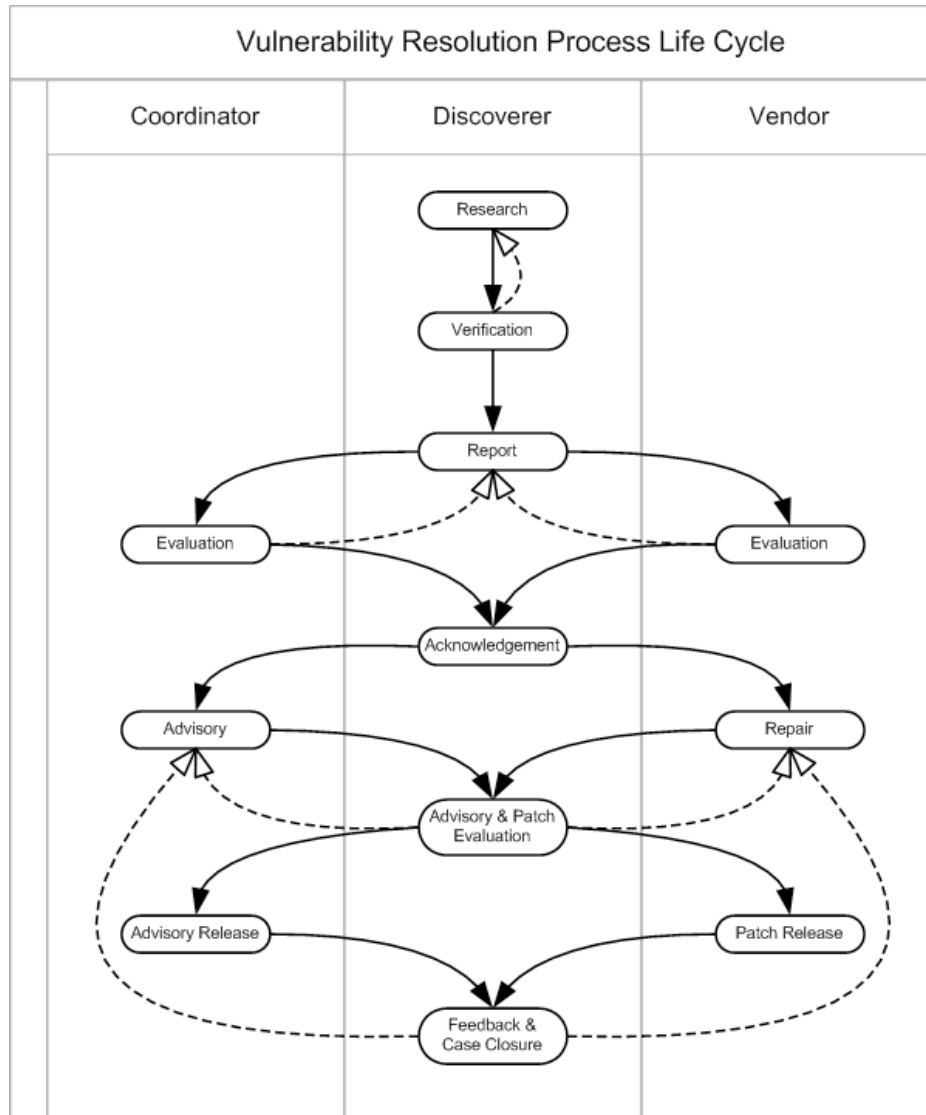
The following IPA manual also contains some refers for do/don't of a disclosure:

http://www.ipa.go.jp/security/ciadr/vuln_announce_manual_en.pdf

B.6 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.7 Coordinators Recognized Globally

The following list identifies vulnerability coordinators which are known globally.

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] "Vulnerability Disclosure Framework" by NIAC <http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf>
- [2] "Full Disclosure Policy (RFPolicy) v2.0" by Rain Forest Puppy <http://www.wiretrip.net/rfp/policy.html>
- [3] "Responsible Vulnerability Disclosure Process" by Steve Christey and Chris Wysopal (<http://tools.ietf.org/draft/draft-christeywysopal-vuln-disclosure/draft-christeywysopal-vuln-disclosure-00.txt>)
- [4] CERT/CC Vulnerability Disclosure Policy http://www.cert.org/kb/vul_disclosure.html
- [5] VULDEF: The Vulnerability Data publication and Exchange Format data model <http://jvnrss.ise.chuo-u.ac.jp/jtg/vuldef/index.en.html>
- [6] CAIF - Common Announcement Interchange Format <http://www.caif.info/>
- [7] ISO CD 29100 – Information technology – Security techniques – Privacy framework