Vulnerability Disclosure Guideline for Software Developers

Excerpt of Information Security Early Warning Partnership Guideline Appendix 5

Contents

July, 2009

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

JAPAN COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER

JAPAN ELECTRONICS AND INFORMATION TECHNOLOGY INDUSTRIES ASSOCIATION

COMPUTER SOFTWARE ASSOCIATION OF JAPAN

JAPAN INFORMATION TECHNOLOGY SERVICES INDUSTRY ASSOCIATION

JAPAN NETWORK SECURITY ASSOCIATION

1. Introduction

In terms of quality and reliability assurance, it is important for vendors and individuals who develop software ("the software developers") to provide secure products to their users, such as home users and system integrators ("the users"). A product that has been developed through thorough security design, however, could still contain security holes ("vulnerabilities").

If the software developers do not disclose information knowing their products have vulnerabilities and conceal the damage they may cause, or provide insufficient or even false information, it could put information assets or social activities of the users at risk. The software developers should voluntarily take necessary action as quickly as possible and offer accurate vulnerability information to the users.

The current situation, however, suggests that some software developers may not have experience in vulnerability disclosure and end up in providing incomplete information in an inappropriate way and preventing the users from obtaining necessary information.

The primary purpose of this guideline is to present an advisable policy and procedure to assist the software developers in providing essential vulnerability information to those users in need.

2. Vulnerability Information: Provide What Users Need

When the software developers provide vulnerability information to the users, they should be aware of what information the users need to know. If the software developers provide a security patch without adequate information, it may cause trouble for the users. Here are the kinds of information the users likely want to know and why.

(1) The Product Name and Version

First of all, the users are most likely eager to know whether or not a given vulnerability affects them. Therefore, it is desirable to provide vulnerability information in such a way that the users can easily identify the product names and versions affected by the vulnerability.

(2) The Date of Publication

On Web sites, old information can look like new. The newer the vulnerability information is, the higher the chances that it affects the users. On the other hand, if the information is moderately old, the vulnerability may have already been patched. Provide the date on which you published the vulnerability information to save the users from possibly checking out the information about the vulnerability they have already taken care of.

(3) Threats

When vulnerability information is disclosed, some users let it go if it poses low threat and take action only if it is highly dangerous. Therefore, it is encouraged to provide the users with information on what could happen in concrete terms if they do not apply the security patch.

(4) Workarounds

There may be the cases where the users cannot apply a security patch. If some workarounds to avoid or withstand attacks are available, they should be let known to the public. If the software developers provide only a security patch and no detailed information on the vulnerability, workarounds are difficult to work out and the users who cannot apply the security patch may be put at risk. If the software developers are aware of some workarounds, they should provide the information on how to implement them properly.

(5) Other Information

Besides the information provided by the software developers, the users often try to check out the supplemental information in order to assess the severity and urgency of the vulnerability. It is important to provide these information for reference.

3. What to Provide: Vulnerability Information Items and Publication Examples

This chapter gives a list of information items that should be included in vulnerability information when the software developers disclose the vulnerability on their web site and presents a recommended publication example as well as a few undesirable ones.

3.1. Items to Be Included in Vulnerability Information

What information the users want to get may differ depending on whether they are system integrators or home users. The system integrators tend to put weight on detailed information about the threats and workarounds, while home users more likely appreciate information on how to check if they are using the affected products or a jargon-free, easy-to-understand description to fix the problem. It is recommended that the software developers analyze the expected user base based on the nature of their products and provide information in an appropriate focus and layout.

The following shows a commonly preferable order to publish vulnerability information item by item.

3.1.1. Title

Include the product name in the page title so that the users who look for vulnerability information via search engines could get a hit. Put the vulnerability ID and the name of the vulnerability in the title as well to distinguish each vulnerability because a product may have multiple vulnerabilities; one may have already been found in the past or may be found in the future. In addition, indicate clearly that it is vulnerability information for those who get to the page directly from the external web sites.

3.1.2. Overview

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

3.1.3. Affected Products

Give a list of the affected products/versions and explain how to check the version of these products.

3.1.4. 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.

3.1.5. Threats

Provide information to assess the severity of the vulnerability. For example, what may happen if the vulnerability is exploited in attacks, the level of risk and the probability an attack succeeds.

3.1.6. Solution

Provide information on how to install the fixed product, update and apply a security patch.

3.1.7. 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.

3.1.8. References

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

3.1.9. Credit

Some software developers put acknowledgement in vulnerability disclosure to credit the contributor for discovering and reporting the vulnerability.

3.1.10. Revision History

Clarify the date on which the vulnerability was first known to the public. If revised, add when and what was updated.

3.1.11. Contact Information

Provide contact information in case the vulnerability information is unclear or the security patch has caused some trouble.

3.1.12. Publication Examples

The following recommended format for vulnerability disclosure has been prepared in reference to Consumer Products Recall Handbook (listed in 5. References) as an example where the software developers cannot specify the expected user base and settle to provide the information to the public in general.

- **Example of Recommended Format for Vulnerability Disclosure**

Security Vulnerability Information > Product: XYZ

IPASA2007-001: Buffer Overflow Vulnerability in XYZ

Date First Published: Jan. 1, 2007
Last Updated: Jan. 9, 2007

■Overview

A buffer overflow vulnerability has been found in the XYZ version 3.02 and earlier. When exploited, this vulnerability may allow a remote attacker to execute arbitrary code on the computer running XYZ.

Apply the security patch to the affected products listed below.

■Affected Products

This issue affects the following products:

Product Name XYZ
Affected Versions
1.5.4 (for Windows XP SP2) and earlier
1.5.4 (for Linux) and earlier

How to check the version information of XYZ.
1, Start XYZ, go to the Help menu and click Version Information.
2. The version information is shown on the last line in the popup window (Figure1).

[Figure1（XYZ Version Information）inserted here]

■Description

XYZ has a decompression function for compressed files. The decompression function, provided as part of data management services in the Data Application Suite, is vulnerable to buffer overflow. This allows a remote attacker to execute arbitrary code over the Internet.

■Threats

If an attack succeeds when the software is running under the privileges of the system administrator, a remote attacker could gain full control over the computer. The attacker could execute arbitrary commands, such as installing malicious programs and modifying/deleting data, with the administrator privileges.

・IPASA2007-001 Technical Information

■Solution

If you use the XYZ version 1.0.0 and earlier, uninstall it and newly install the fixed product. For those who use XYZ later than version 1.0.0, apply the security patch.

For installation guidance, see readme.txt supplied in each program.

Product Name XYZ
Security Patches for Download
1.5.5 patch.zip (for WindowsXP SP2) 2007.1.4
1.5.5 patch.tgz (for Linux) 2007.1.4

・The configuration files listed below will be replaced in the process
xxxxx.cfg、yyyyy.dif

■Workarounds

The following action could possibly mitigate the vulnerability.

・Workaround

To mitigate the effect, set the filtering rules using the IP address filtering feature or a router to limit IP addresses that can establish connection to the ports used in administrative operation in XYZ to the trusted ones.

■References

JVN#12345678 Buffer Over Flow Vulnerability in XYZ

■Credit

Credit goes to Mr. John Doe for finding this vulnerability.

■Revision History

2007.01.4 The page published.
2007.01.9 Add technical information to the Threats section for the cases where the software is running under the lower privileges.

■Contact Information

Tel: 123-456-7890 (Weekdays 10:00 – 17:00)

Email: example@example.co.jp

- **Example of Undesirable Format for Vulnerability Disclosure (1)**

XYZ Update

Recently, we have learned that the decompression function in our XYZ may show some performance instability in some rare situations.

We hereby provide update program for XYZ although this occurs in the limited use environment.

We are committed to help the users and continue our efforts to secure our products.

■Update Program

XYZ 1.5.5 (for Windows)　　XYZ 1.5.5 (for Linux)

What's Wrong with This Example

- It is unclear for the users what the purpose of this announcement is, which is supposed to ask the users to promptly update the software to fix the vulnerability.
- The format looks like ordinary marketing news often sent to the users, and thus fails to attract needed attention from the users and to raise a flag that this is a vulnerability information.
- It is undefined how dangerous the vulnerability in question is, thus the users cannot make an informed decision whether they should take action as soon as possible.
- The users cannot take action since no information is available regarding how to install update program.
- The users cannot confirm the date of publication, and thus cannot get a clue whether or not they may have taken care of the vulnerability already.

- **Example of Undesired Format for Vulnerability Disclosure (2)**

XYZ Release Notes

2007.1.4　　Version 1.5.5

・Add a header editing function to the email sending function

・Correct the issue in which buffer overflow occurs when a too long file name is send to the file upload function.

・Correct minor bugs.

2006.11.28　Version 1.5.4

・Added the file upload function.

.....

What's Wrong with this Example

- It is difficult for the users to judge whether the announcement aims at simple functional enhancement or the vulnerability issues are addressed as well.

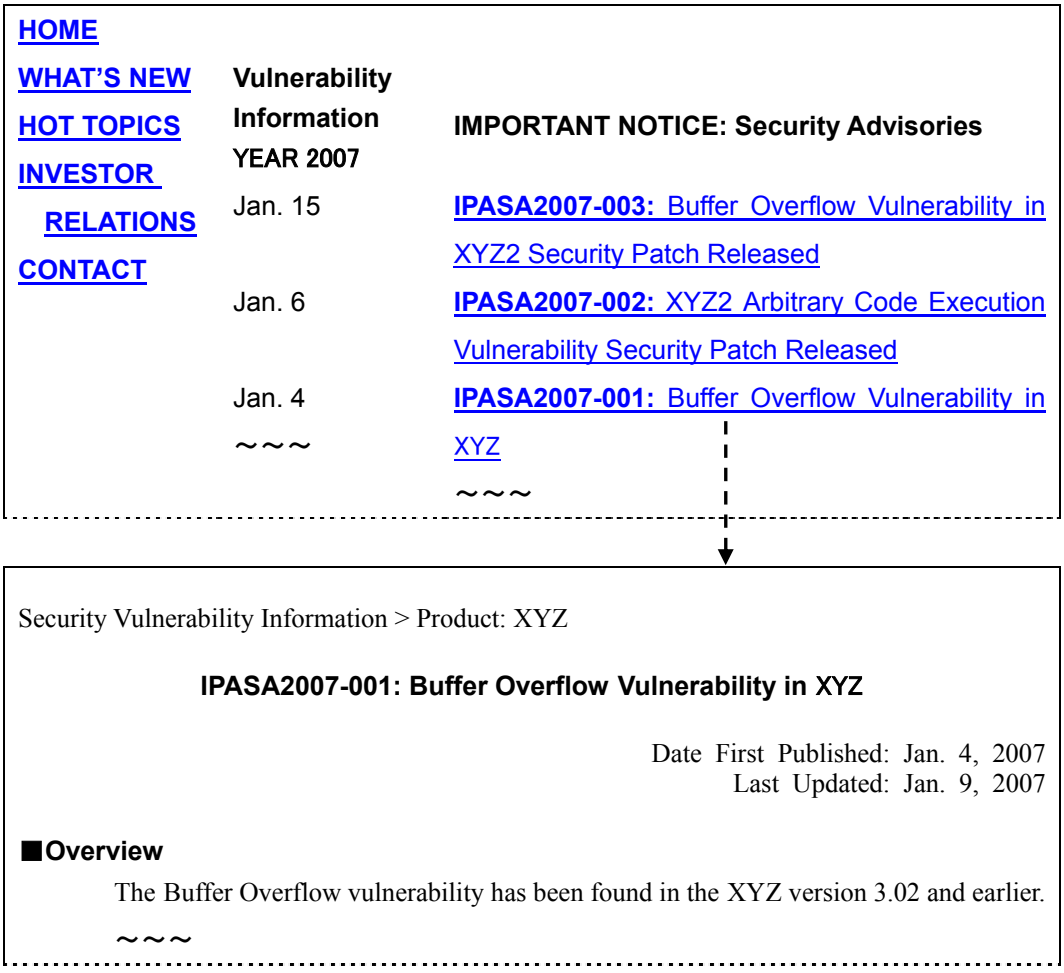
4. How to Provide: Navigation to Vulnerability Information on the Web Site

This chapter gives advice on how to guide the users to vulnerability information from its Home page on their web site. Here we illustrate a recommended way and undesirable way to do it through the examples.

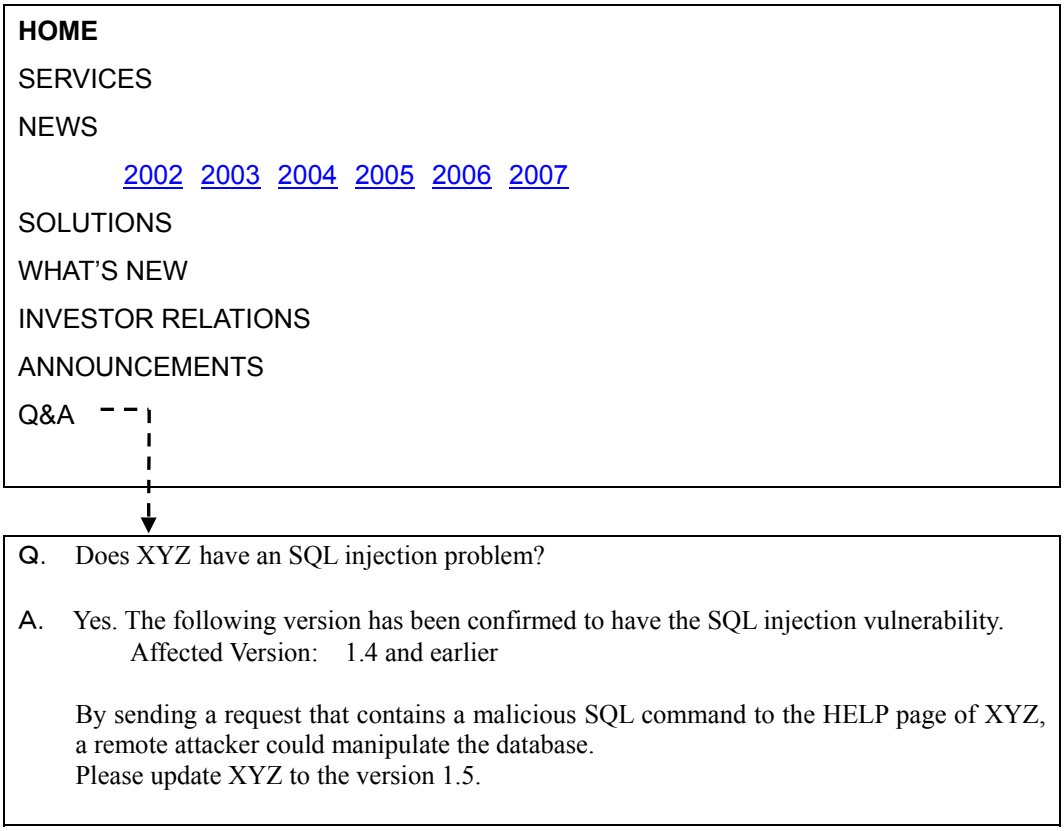
The Good Web Site Design for Vulnerability Information:

- 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 just like 1.3.10 (Revision History).

- **Example of Recommended Web Design**



- **Example of Undesired Web Design**



What is Wrong with This Example

- Vulnerability information is mixed in other information category（Q&A in this case）.
- Since this vulnerability information is buried among FAQs, it is not clear that this is a vulnerability information.
- Most likely, the users would not anticipate that they will find vulnerability information here.
- The users have no way of knowing when the information was published.

5. References

Ministry of Economy, Trade and Industry（METI） Product Safety Division, *Consumer Products Recall Handbook*, (Appendix 2 Press Release Example (Good Press Release)), May 2002, p. 47
http://www.meti.go.jp/policy/consumer/seian/contents/recall/handbook.pdf (in Japanese)

・Background

In the recent years, the number of vulnerabilities found in software or web applications in Japan has been steadily increasing and the raise in unauthorized access or computer viruses exploiting these vulnerabilities has caused serious damage, such as halt in enterprise operation, loss of information assets and disclosure of personal information.

To set the policy how to handle vulnerability information when a vulnerability is found, the METI Directive “the Standards for Handling Software Vulnerability Information and Others” and “Information Security Early Warning Partnership Guideline”, which explains a recommended procedure to the parties involved in vulnerable disclosure, have been issued.

This document is the excerpt of Appendix 5 from the Guideline (last revised on July 8, 2009). The intended readers are the software developers and the guideline aims to provide a possible policy that would help them and encourage proper disclosure of vulnerability information.

We ask the software developers refer to this document to make sure to provide necessary information to the users when disclosing vulnerabilities.

This document is free to distribute without limitation and available for download at:

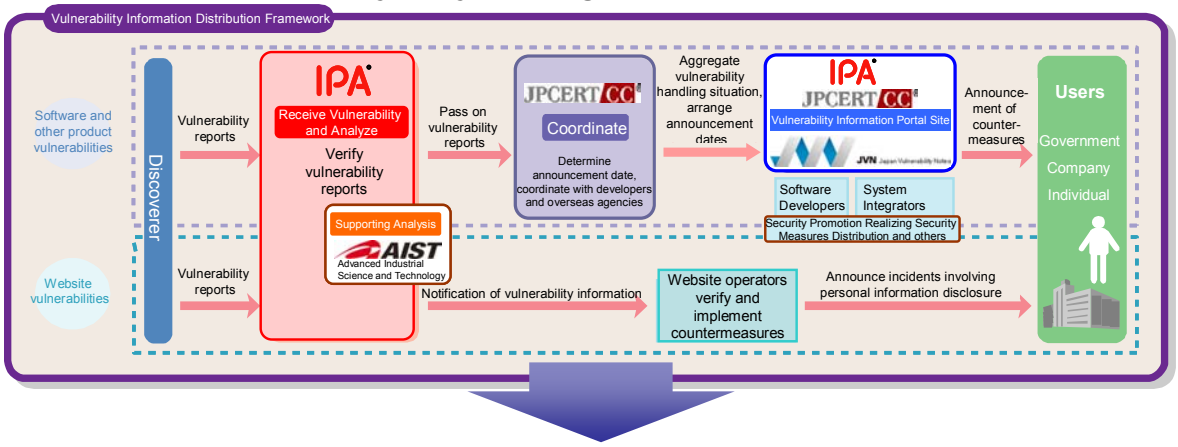
http://www.ipa.go.jp/security/english/third.html

http://www.jpcert.or.jp/english/vh/guidelines.html

http://www.ipa.go.jp/security/ciadr/partnership_guide.html (in Japanese)

http://www.jpcert.or.jp/vh/index.html#link_japan (in Japanese)

・Framework for Handling Vulnerability-Related Information
- Information Security Early Warning Partnership -



Expected Effects

1. Promotion of vulnerability countermeasures taken by product developers and website operators
2. Prevention of inadvertent disclosure of vulnerability information and vulnerabilities being neglected
3. Prevention of critical system outage and critical information leaks including personal information

IPA: Information-technology Promotion Agency, Japan, JPCERT/CC: Japan Computer Emergency Response Team Coordination Center, AIST: National Institute of Advanced Industrial Science and Technology

・Contact Information

Security Center, Information-Technology Promotion Agency, Japan（IPA）

2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan

http://www.ipa.go.jp/security/ TEL: +81-3-5978-7527 FAX: +81-3-5978-7518

Japan Computer Emergency Response Team Coordination Center（JPCERT/CC）

Hirose Bldg. 11F, 3-17 kanda-nishikicho Chiyoda-ku, Tokyo 101-0054, Japan

http://www.jpcert.or.jp/ TEL : +81-3-3518-4600 FAX : +81-3-3518-4602

Vulnerability Disclosure Guideline for Software Developers

— Excerpt of Information Security Early Warning partnership Guideline Appendix 5 —

[Publication] May 30, 2007 First Edition, July 29, 2008 English Translation First Edition

July 8, 2009 Second Edition, Third Printing, July 8, 2009 English Translation Second Printing

[Editor] Information System Vulnerability Information Handling Study Group

[Organizer] Information-Technology Promotion Agency, Japan