



ISO/IEC JTC 1/SC 27 **N 6639**

ISO/IEC JTC 1/SC 27/WG 3 **N 934**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: other

TITLE: Information technology – Security techniques – Responsible vulnerability disclosure – JPCERT Presentation

SOURCE: 36th SC 27/WG 3 meeting

DATE: 2008-04-15

PROJECT: 29147

STATUS: This document was available at the above-mentioned meeting. It is being circulated for information.

ACTION: FYI

DUE DATE:

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

MEDIUM: Server

NO. OF PAGES: 1 + x

Possible scope of discussion on Responsible Vulnerability Disclosure

JPCERT/CC
Toshio Miyachi

Vulnerability handling in Japan

- Japan has a formal vulnerability handling framework based on a government ministry order since July 2004, which is called “Information Security Early Warning Partnership,” in order to improve the level of social information security.
- The ministry order is strongly recommending a person who finds a vulnerability reporting it to the designated coordinator and keeping it in secret until date which the coordinator specifies.
- In the framework JPCERT/CC has handled vulnerabilities as the coordinator with IPA of Japan and foreign partners such as CERT/CC in U.S. and CPNI in U.K.

Lifecycle model of vulnerabilities

((Embryonic phase))

1. The developer of the product work on it for deep analysis and confirms that it is a vulnerability if in the case.
2. The developer develops a patch or a new version of the product to fix it or a workaround to avoid attacks, or decides to terminate the life of the product.

((Dissemination phase))

3. The developer, the finder and the coordinator releases the vulnerability information for public.
4. The user of the product implements one of solutions of the vulnerability.

What is our scope?

- The responsible vulnerability disclosure should focus only the dissemination phase.
- We encounter many difficult issues in the embryonic phase such as:
 - The definition of vulnerability
Is it a vulnerability or just a bug?
 - The policy of vulnerability disclosure
Immediate release of the information?
Or should we wait until a patch becomes available?
 - Stakeholders with very different viewpoints
 - Developer, finder, user, coordinator, and so on.

Vulnerability handling

needs to consider many aspects (1/2)

- Categories of products:
 - Software for personal computers and IP routers
 - Relatively easy to handle.
 - Software component for information systems of large scale such as a banking system
 - It takes long time for testing before patching.
 - Software for control systems (so-called SCADA)
 - Patching itself is not an easy task.
 - It takes long time for testing before patching.
 - Firmware for consumer electronics products
 - Patching itself is not an easy task.
 - Awareness of consumers and shops are generally low.

Vulnerability handling needs to consider many aspects (2/2)

- Source of vulnerability
 - Specification of technology
 - A standardization body is a stakeholder.
 - It takes long time to fix it.
 - Module developed by a product vender
 - Relatively east to handle.
 - Common module used by many product venders
 - Not so easy for each vender to handle.
 - Multi vendor coordination is not easy.
 - Inappropriate default setting
 - Relatively easy to handle.
 - Combination of software modules such as a browser and its plug-in

Conclusion

- We should carefully define our scope of work as sharp as possible.
- A wider scope is fascinating conceptually, but ...
- The Japanese national body is willing to contribute to the new work item with the four year experience of JPCERT/CC and IPA on vulnerability handling in Japan.