

**Proposed Guidelines**  
**for the Co-Ordinated Disclosure of Software Vulnerabilities Affecting Multiple Vendors’**  
**Products Through Third Party Co-Ordination Centers**

**Key Objective of the Guidelines**

These guidelines pertain to situations when a third party coordinating entity undertakes to co-ordinate with multiple vendors the public disclosure of vulnerability (as that term is defined below). The vendors elect to work with such a Coordinator for the common benefit of advising affected customers in an appropriate, reliable and timely manner.

It is presumed that over time, there will be an increase in the number of third party co-coordinators whose mission will be to address such matters, particularly in emerging worldwide internet-related markets. These guidelines do not attempt to cover *all* aspects of the public reporting function; however, they do attempt to outline certain key concepts and practical requirements that can better enable this kind of public reporting process.

**A. Definitions**

As used in these guidelines, the terms below have the following meanings:

“**Public**” denotes entities outside of a vendor. That can represent public at large (e.g., public mailing alias like Bugtraq) or a closed alias for customers of a particular vendor.

“**Vendor**” means a private or public corporations, partnerships or other for-profit business entities.

“**Third party Coordinator center**” or “**Coordinator**” means a third party unaffiliated with any particular vendor, and an entity that does not have any kind of vested interest in any particular vendor’s products. Ideally, the Coordinator should be “neutral” that is, not tied to any particular government(s) or vendor, and preferably be a non-profit organization to avoid potential conflict of interest. It can also means an organization composed of a consortium of vendors who, while having a vested interest in the process, have agreed to a uniform process for managing of vulnerability issues.

“**Vulnerability**” is defined as a set of conditions that leads or may lead to an implicit or explicit compromise of the confidentiality, integrity, or availability of an information system. Examples of the unauthorized or unexpected effects of vulnerability may include any of the following:

- Executing commands as another user
- Accessing data or services in excess of specified or expected permission
- Posing as another user or service within a system
- Causing an abnormal denial of service
- Inadvertently or intentionally destroying data without permission
- Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message
- Committing a fraud

Common causes of vulnerabilities are design or coding mistakes in software and hardware, botched administrative processes, lack of awareness and education in information security, and advancements in the state of the art or improvements to current practices, any of which may result in real threats to mission-critical information systems.

**B. Common Points for Vendors and Coordinators**

1. **English as the Common Language.** Vendors and Coordinators are expected to be able to use English as the common language for all written and verbal communications when coordination is being done on international basis. English would be used for the published, public reporting of vulnerabilities. Any additional language usage may be helpful in a given geography, as long as translations into local language do not cause confusion or conflict with the English version.
2. **Adequate Resources to Address Issues Outside of “Normal” Business Hours.** Threats of exploitation and exploitations can occur anywhere in the world at any time. A best practice for those engaged in the “business” of managing internet security today is premised on having adequate flexibility and resources to address such threats, as they may arise. Vendors and Coordinators should have capabilities to operate and promptly respond to a given vulnerability coordination scenario either on 24x7x365 basis or otherwise have resources available to adequately handle emergency or other situations that can require support and coordination outside of normal daytime office hours.
3. **The Parties Must Work Together In Good Faith.**

Vendors and Coordinators must operate at all times throughout the vulnerability disclosure process in good faith, a key linchpin for any successful, coordinated multiple vendor disclosure process. The Coordinator must, in good faith, timely notify all potentially impacted vendors of a discovered vulnerability and, upon timely response from vendors, then set a time schedule for public disclosure of the vulnerability that is reasonable under the circumstances; that is, a time by which vendors should have developed a software patch, workarounds or other remedies for their product(s). Vendors must also act in good faith to timely assess the impact of a discovered vulnerability to their products and respond to the Coordinator’s inquiries.
4. **The Need to Keep Undisclosed Vulnerability Information Confidential.**

Prior to the time when the Coordinator publicly reports of the discovered vulnerability, all vendors in receipt of the vulnerability information should treat such information confidentially. The key underlying need for all parties to maintain such confidentiality is the understanding that the inadvertent public disclosure of such information before the co-ordinated public disclosure can potentially place all vendors’ customers and product users at risk of a potential exploitation.

For example, prior to the Coordinator’s scheduled public disclosure of the vulnerability, a Coordinator usually will provide vendors information about the nature of the particular vulnerability (or in some cases, even provide a copy of the exploit code itself) so that the vendors can properly analyze the vulnerability and then create patches or other remedies.

Both the Coordinator and each vendor who participates in the disclosure process should keep the vulnerability information confidential at least until the time of the Coordinator’s scheduled public disclosure, and absent any countervailing legal obligation to disclose

such information to a third party. Certain kind of information, such as actual exploit code, may be kept confidential even after the public disclosure.

However, it must also be recognized that in instances when either a vendor or the Coordinator becomes aware that the vulnerability is being exploited or is imminently subject to being exploited, the vendors and the Coordinator may need to take swift, definitive action to advise customers and/or issue public notification of the matter. In such exceptional cases, vendors should use all reasonable efforts under the circumstances to advise as much advanced notice to the Coordinator, who should likewise quickly notify the other potentially impacted vendors.

Coordinators should have the right to not work with a vendor who has failed to maintain confidentiality and to report to other vendors any instance when confidentiality has been threatened or actually compromised.

Each vendor's receipt and internal management of such confidential information should be done under strict confidentiality terms. The Coordinator must likewise keep all information pertaining to any vulnerability confidential and not disseminate it except through the scheduled public reporting process. This does not preclude internal information sharing that is necessary for the Coordinator's operation and internal reporting. It must operate on the same need-to-know policy as vendors do. Non-public information must not be disclosed to non-vendors and end users.

5. **Identified, Trained and Knowledgeable Personnel.**

The business of addressing vulnerabilities requires having adequately trained and knowledgeable vendor and Coordinator personnel who can address the technical, operational, PR, legal and other issues associated with such process. It is also important that such personnel are *known to* the respective parties, and that an appropriate identity verification system be established.

6. **Secure Communication Channels and Encryption Capabilities.**

Both vendors and Coordinators *must* have the capability to exchange confidential information using strong encryption and per other secure modes of communication.

C. **Key Guidelines and Responsibilities for Vendors**

- (a) Vendors recognize the need to continually work to improve their internal processes, public reporting and coordinating processes in an effort to minimize the impact that vulnerabilities may have upon their respective customers. It is important for vendors to strive to establish and enhance workable framework that enables Coordinators to publish vulnerability information for the benefit of the vendors' customers so that such customers can find and effectively use such information.
- (b) A significant level of cooperation and trusted communications must occur by vendors with the Coordinator and among vendors who are engaged with the Coordinator, in order for the Coordinator to successfully manage the public reporting process. To that end, vendors should strive to respond as quickly as possible under given circumstances to the Coordinator's legitimate requests and inquiries.

## Guidelines for Vendor – Coordination Centers Relationship rev1.0

- (c) Vendors should cooperate with each other as is necessary for the primary purposes of enabling the Coordinator to timely release information regarding a discovered vulnerability.
- (d) Vulnerabilities that may affect more than one vendor's products should, in most instances, be publicly disclosed through a Coordinator.
- (e) Vendors retain the right to make their own decisions regarding the scope and nature of their coordination efforts with Coordinators and other vendors. However, vendors must disclose sufficient information to enable effective coordination by the Coordinator, which should include providing the Coordinator *at least* the following two essential pieces of information:
  - Whether the identified vulnerability impacts the vendor's products; and, if so:
  - The date when the vendor believes it will have a software patch or other type of fix available for public release.

Other helpful (but non-essential) information for vendors to provide may include any available or potential workarounds, or assessment of the character of the vulnerability.

- (f) Vendors should not be required to reveal certain details about the vendor's products or internal processes that are extraneous to the Coordinator's role. For example, a vendor may withhold information about how a vulnerability impacts its products, or which products it impacts, or the internally identified activities it is undertaking to timely address the vulnerability in light of the Co-coordinator's articulated scheduled date for public disclosure. Alternatively, a vendor can provide Coordinator with instructions on which details can be shared and under which circumstances.
- (g) Vendors may, in their discretion, disclose vulnerability details to other trusted vendors whose product(s) depend upon and/or are negatively impacted by, the identified vulnerability. Vendors may elect not to disclose which other vendors they have contacted. For example, after becoming aware of a vulnerability, a vendor may elect to contact other vendors in order to address any interoperability or other technical questions. A product may incorporate one or more constituent components (parts, components, software modules or libraries) that are provided and maintained by OEMs or other third parties. Another example is when a vulnerability may impact the interoperability with products from other vendors. In such cases, a vendor must work with such third parties in order to provide the necessary remedy for its product.
- (h) Vendors should establish internal capabilities/resources to sufficiently handle sensitive information and the public reporting of vulnerabilities, including the capability to appropriately participate in a coordinated Public Disclosure managed by a Coordinator. At a minimum, vendors should have personnel with contact information that is available to the Coordinator and other vendors. Global vendors, and ones with sufficient resources, should consider having a dedicated vulnerability handling team available and operational on a 24x7 basis.
- (i) Under usual circumstances when vulnerability is to be disclosed through a Coordinator, a vendor who is participating in the coordinated disclosure should not unilaterally publicly disclose information about the vulnerability *prior to* the coordinated public disclosure date.

**D. Key Guidelines and Responsibilities for Coordination Centers**

- (a) An important task of Coordinators is to coordinate with multiple vendors regarding the timely public disclosure of a discovered vulnerability. The Coordinator should collect from vendors adequate information in order to establish an appropriate time line for disclosure. The Coordinator should not *unilaterally* make decisions to publicly disclose vulnerability information that do not take into account the input/feedback from vendors; any such decision should be made only if a representative set of vendors are first consulted.
- (b) Coordinators must be capable of reaching numerous potentially impacted vendors on a worldwide basis.
- (c) Coordinators should have means to provide adequate 24x7 coverage, particularly for handling emergency situations. Their representatives should be easily reachable by vendors and good faith efforts should be made to reach vendor personnel directly in any kinds of emergency situations (i.e. leaving only voicemails is obviously inadequate).
- (d) The Coordinator should not pre-disclose non-public vulnerability information to third parties (i.e. individuals or entities *other than* the vendors who are impacted by the vulnerability), unless prior to any disclosure to a third party the Coordinator:
  - (i) undertakes a good faith assessment that the disclosure of such information to a third party is absolutely required *for effective coordination purposes*; and
  - (ii) notifies the vendor from whom Coordinator originally received the information that Coordinator seeks to disclose to the third party; and
  - (iii) obtains written assurance from the third party that the third party shall treat and hold the information it receives from the Coordinator in strict confidence on a need to know basis (prior to the time the vulnerability information is published by the Coordinator) and will identify its authorized personnel to Coordinator.
- (e) The steps for disclosing information to third parties (identified in section c above) are not intended to preclude the Coordinator’s own internal information sharing that is necessary for the Coordinator’s operation and internal reporting functions to perform their regular duties.
- (f) When coordinating multiple vendors Coordinator should provide a list of all other vendors involved on that particular issue. Ideally, such a list should include the name and email address or phone of each vendor’s contact person; however, at a minimum, a list of vendor names should be available. At very least Coordinator must disclose the fact that multiple vendors are affected. If given permission, Coordinator should pass identity of the person/organization that discovered the issue to all affected vendors.
- (g) Coordinators should publish their disclosure and information handling policies and practices, particularly regarding the timing, scope, and content of publishing vulnerability reports, what sanctions Coordinators may take against a vendor who does not “play by the rules” and the Coordinator’s affiliations with any government or other organizations.