Guidelines for Security Vulnerability Reporting and Response

Organization for Internet Safety

Version 2.0
01 September 2004

Table of Contents

Guidelines for Security Vulnerability Reporting and Response

1 Introduction

1.1 Purpose

Security vulnerabilities in software systems pose a constant threat to computer users, the Internet, and the critical infrastructures that depend on it. The fact that security vulnerabilities exist at all is, of course, the core problem, and building secure software systems must remain the industry's goal. However, because security vulnerabilities do occur, it is vital that information systems be protected against them as effectively as possible. A variety of models for doing this have been advocated.

This document provides a reference process embodying best practices associated with one such model, which is characterized by close collaboration in good faith between the person or organization who identifies a vulnerability and the person or organization responsible for maintaining the product in which it occurs. This model can provide two benefits:

- 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, high-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.

The guidelines described herein are intended to be suitable for use by companies, individuals, and organizations with a variety of resources and expertise in computer security. They are intended to be agnostic regarding the software development model used, and be appropriate for adoption worldwide. Additional information about the background of these guidelines, the Organization for Internet Safety, and its goals in developing them is available at http://www.oisafety.org.

1.2 Definition of a Security Vulnerability

For the purposes of these guidelines, a security vulnerability is a flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy[1].

1.3 Use of this Reference Process

Companies, individuals, and organizations that wish to follow the vulnerability-handling model detailed herein may use this reference process in whole or in part. The authoritative version of these guidelines will be hosted at http://www.oisafety.org/guidelines/secresp.htm, and will be available for use as a reference by the general public.

[1] Such documentation is sometimes published directly, as part of a product's associated documentation. In other cases, it may be provided as collateral information, as in the case of the Target of Evaluation for products evaluated under the Common Criteria system. Even in cases where neither of the above are done, user guides and other documentation typically describe a product's intended operation, including its intended security operation.

For clarity, companies, individuals, and organizations that adopt these guidelines should provide a written security response and/or security reporting policy at an easily discoverable location on their web site. The Security Policy should note that it is based on these guidelines, and clearly note all areas where their process differs from this one.

1.4 Scope

The reference process provided herein applies to software products and software/firmware components of hardware products that are distributed by vendors to others. While it is important that vendors minimize the occurrence of security vulnerabilities in the first place, identifying and prescribing the engineering practices to do this is beyond the scope of this document. Similarly, although security vulnerabilities can and do occur as the result of flaws in hardware products, network architectures, operational procedures, and other factors, the process by which these should be identified and remedied is beyond the scope of this document.

1.5 Limitations

The purpose of this document is to describe a voluntary process for reporting and resolving reports of potential security vulnerabilities. Nothing in this document shall create any legal rights or obligations. Similarly, in cases where the stipulations of this document conflict with applicable law or contractual obligations of any party, the law or such obligations shall have precedence.

The guidelines discussed in this document are not intended to mandate specific business practices. Participants should resolve any such conflicts between these guidelines and their business practices in a way that represents reasonable efforts to safeguard customers, the Internet, and the critical infrastructures that depend on it.

1.6 Identifying Requirements

In the document that follows, requirements are provided within sections titled “Requirements.” Every requirement is numbered, and identifies the requirement and the party or parties responsible for carrying it out. The use of the word “shall” in a requirement means that the action it describes is affirmatively required by the guidelines. The use of the word “may” means that the action is neither required nor prohibited.

Text outside the Requirements sections consists of background, contextual information, recommendations, and examples, but constitute requirements only insofar as they are also contained a Requirements section. Similarly, figures are provided to aid readers in understanding the process, and do not provide an exhaustive listing of requirements.

1.7 Process Maintenance

The Organization for Internet Safety shall review these guidelines no less than biennially and propose amendments that remedy shortcomings, improve the process, or reflect feedback from the people and organizations that use it. Comments, suggestions, and feedback about the process are welcome, and should be directed to feedback@oisafety.org.

2 Process Overview

2.1 Participants

Although additional participants may be involved in this process, the primary participants are:

- **The Finder**. The security researcher, customer, or other interested person or organization who identifies the vulnerability.

- **The Vendor**. The person, organization, or company that developed the product, or is responsible for maintaining it.
- **Coordinator**. An optional participant that serves as a proxy for the Finder and/or Vendor, assists with technical evaluations, or performs other functions to promote the effectiveness of the security response process.
- **Arbitrator**. An optional participant that adjudicates disputes between the Finder and Vendor.

Although computer users are the ultimate beneficiaries of this process, they are not listed among the participants. This is because their role in maintaining security begins at the point where this process terminates: when a suspected vulnerability has been investigated and confirmed, and a remedy is available.

2.2 Phases

As shown in Figure 1, the basic steps of the process are:

- **Discovery**. The Finder discovers what it considers to be a security vulnerability (the Potential Flaw).
- **Notification**. The Finder notifies the Vendor and advises it of the Potential Flaw. The Vendor confirms that it has received the notification.
- **Investigation**. The Vendor investigates the Finder's report in an attempt to verify and validate the Finder's claims, and works collaboratively with the Finder as it does so.
- **Resolution**. If the Potential Flaw is confirmed, the Vendor develops a remedy (typically a software change or procedure) that reduces or eliminates the vulnerability.
- **Release**. In a coordinated fashion, the Vendor and the Finder publicly release information about the vulnerability and its remedy.

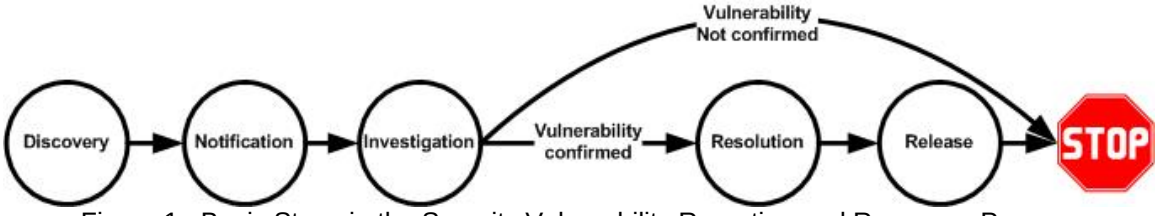

Figure 1. Basic Steps in the Security Vulnerability Reporting and Response Process

2.3 Timeline

There is no single universally appropriate timeframe for investigating and remedying security vulnerabilities. Instead, the Finder and Vendor must work together to develop a target timeframe that balances the risk posed by a particular vulnerability versus the engineering challenges associated with thoroughly investigating and effectively remedying it. By convention, 30 calendar days has been established as a good starting point for the discussions, as it often provides an appropriate balance between timeliness and thoroughness.

Within the agreed-upon timeframe, predictable and regular communications occur between the Finder and Vendor. Within a maximum of seven calendar days of receiving the Finder's report, the Vendor acknowledges its receipt. Thereafter, the Vendor provides status updates every seven calendar days, unless a different interval has been mutually agreed to. If the Finder does not receive these communications, it sends a request to the Vendor, which the Vendor responds to within three calendar days.

Once the investigation is complete and a remedy has been delivered, one additional timeline remains, regulating the release of details that could lead directly to attacks if misused. The

Finder and Vendor observe a 30-day grace period beginning with the release of the remedy, during which they provide such details only to people and organizations that play a critical role in advancing the security of users, critical infrastructures, and the Internet. Upon the expiration of the grace period, these details can be shared more broadly.

2.4 Security

Because of the risk security vulnerabilities pose, it is important that adequate security measures be observed throughout the process described herein. Two types of security measures are particularly important:

- **Communication Security.** These measures enable the Finder and Vendor to communicate securely with each other during the process of identifying, investigating, and remedying a vulnerability. This is typically provided through the use of encrypted email, although other measures such as secured web sites can also be used.
- **Information Assurance.** These measures allow consumers of security advisories and other published information confirm their origin and authenticity. This is typically provided by digitally signing the publications, although other measures such as hosting on an SSL-protected web site can also be used.

3 Conflict Resolution and Third Parties

3.1 Resolving Conflicts, Deadlocks, and Communication Breakdowns

A key principle of these guidelines is that the best results occur when the Finder and Vendor establish effective communications and maintain them throughout the investigation process, and develop mutually acceptable solutions. Indeed, these guidelines exist to provide a framework in which this can occur easily. Where possible, both Finder and Vendor should work within the process to resolve any conflicts, deadlocks, or communication breakdowns that may arise.

However, this is not always possible. Communications can and do fail. Disagreements, sometimes irreconcilable ones, can and do occur regarding the most effective solution. If the Finder and Vendor find themselves in such a situation, it may be necessary for them to exit this process, either temporarily or permanently, and seek a solution outside its confines.

Such situations typically do not happen because of bad faith on either party's part. More often, communication failures result from benign causes such as human error or temporary e-mail outages; likewise, even reasonable people can disagree about the most appropriate solution to a complex problem. With this in mind, and recognizing the risk that security vulnerabilities pose, several guiding principles should be observed when considering exiting this process:

- **Exit only after exhausting reasonable efforts**. As discussed in Section 3.2 below ("Use of Third Parties"), a Coordinator or Arbitrator can often assist in resolving conflicts.
- **Exit the process only after providing notice**. One party's decision to exit the process should not be a surprise to the other party.
- **Re-enter the process once the deadlock is resolved**. If exiting the process succeeds in breaking the deadlock, a normal working relationship should be resumed if possible, preferably involving returning to this process.

Requirements

3.1.1 If conflicts, deadlocks, or communication breakdowns occur, the Vendor and Finder shall make reasonable efforts to resolve them.

3.2 Use of Third Parties

Security investigations can sometimes be made more effective by the use of people or organizations other than the Finder and Vendor. There is no requirement to use a third party, but in cases where one is used, it should be a person or organization that the Finder and Vendor have agreed to in advance. Characteristics of a good third party include sound judgment, freedom from bias or conflicts of interest, demonstrated security expertise, and discretion. Third parties normally serve in a voluntary capacity, as a service performed in the public interest.

3.2.1 Coordinators

The process of reporting, investigating, and remedying security vulnerabilities can sometimes be expedited by involving a Coordinator, who may serve as a proxy for one of the parties, assist with technical evaluations, or perform other functions to help ensure the success of the security response process. Any person or organization acceptable to both the Finder and Vendor may be used as a Coordinator. It is important to note that the Coordinator's role is not to adjudicate between the parties, but to streamline the investigation and contribute to its quality.

Requirements

3.2.1.1 The Finder or Vendor may propose the use of a Coordinator.
3.2.1.2 A Coordinator shall only be used if both parties consent to its use.
3.2.1.3 The Finder or Vendor may publish in its security response policy a list of Coordinators that it recommends using.
3.2.1.4 The selection of the person or organization who serves as a Coordinator shall require the mutual agreement of the Finder and Vendor.
3.2.1.5 The Coordinator's duties shall be determined by mutual consent of the Finder and Vendor.
3.2.1.6 The use of a Coordinator shall not obligate the Finder or Vendor to be bound by its judgments.

3.2.2 Arbitrators

If the Finder and Vendor reach an irreconcilable disagreement, they should consider involving an Arbitrator, to review each party's claims and adjudicate the dispute. The scope of the Arbitrator's engagement should be clearly spelled out, including whether both parties agree to be bound by its findings.

Requirements

3.2.2.1 The Finder or Vendor may propose the use of an Arbitrator.
3.2.2.2 An Arbitrator shall only be used if both parties consent to its use.
3.2.2.3 The selection of the person or organization who serves as an Arbitrator shall require the mutual agreement of the Finder and Vendor.
3.2.2.4 The scope of the Arbitrator's authority, including whether its judgments are binding, shall be determined in advance by mutual agreement of the Finder and Vendor.

3.3 Exiting the Process

This process exists as a means toward an end, rather than as an end unto itself. In cases where reasonable efforts to resolve conflicts, deadlocks, or communication breakdowns have failed, the goal of protecting computer users, the Internet, and the critical infrastructures that depend on it takes precedence over continuing to follow these guidelines.

Requirements

3.3.1 If an irreconcilable conflict, deadlock or communication breakdown occurs, the Finder or Vendor may withdraw from the use of this process.

3.3.2 If the Finder or Vendor withdraws from this process, it shall exercise reasonable efforts to provide prior notice to the other party.

3.3.3 The Finder or Vendor shall not be required to await acknowledgment of its notice to withdraw from the process.

4 Discovery Phase

Objective: A security researcher, customer, or other interested person or organization discovers what they consider to be a security vulnerability, validates the finding, and prepares a report describing the Potential Flaw.

In Discovery Phase, a finder identifies a potential security vulnerability. Vulnerabilities are found in software products by a variety of individuals, including security consultants, IT professionals, independent researchers, academics, customers, and casual users[2]. They are found both through directed research and normal use.

Before reporting a Potential Flaw to the Vendor, the Finder should perform some due diligence, such as:

- Determining whether the issue has previously been publicly identified and remedied.
- Confirming whether the Potential Flaw affects the product when the current maintenance release or service pack is applied.
- Investigating whether the Potential Flaw affects the default configuration of the product.
- Developing a reproducible method for witnessing the Potential Flaw.

Figure 2. Steps in Discovery Phase

4.1 Vulnerability Summary Report

After validating its findings, the Finder drafts a Vulnerability Summary Report (VSR) discussing the Potential Flaw. The VSR should provide both background and technical information to enable the Vendor to investigate the Potential Flaw. This can include step-by-step instructions, proof-of-concept code, or any other data the Finder believes may help the Vendor confirm its findings.

Requirements

4.1.1 The Finder shall validate its findings and draft a written Vulnerability Summary Report[3] (VSR).

4.1.2 The Finder shall include information in the VSR detailing its intended participation in the investigation. Examples include:

---

[2] Vendors can and do find security vulnerabilities in their own products, and when this happens it is important that the vulnerabilities be remedied quickly and effectively. However, the case where the Finder and Vendor are the same party is significantly different from the case where they are different, and the process for addressing "internal finds" is outside the scope of this document.

[3] A sample VSR is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

- Contact information, if follow-up contact from the Vendor is desired.
- The security reporting process the Finder follows.

4.1.3 The Finder shall exercise reasonable efforts to include ample background information in the VSR. Examples of such data include:

- How the Potential Flaw was found.
- Whether the Finder has published the information or shared it with other parties.
- Any confidentiality requirements that may apply to the report.

4.1.4 The Finder shall exercise reasonable efforts to include sufficient technical information in the VSR to allow the Vendor to confirm the Finder's report. Examples of such information include:

- Products and versions on which the Potential Flaw has been identified.
- Configurations on which the Potential Flaw has been identified.
- Step-by-step instructions, proof-of-concept code, or other data that demonstrate the Potential Flaw.

5 Notification Phase

Objective: The Finder contacts the Vendor and provides the Vulnerability Summary Report discussing the Potential Flaw. The Vendor provides confirmation that it has received the report.

The key activity in Notification Phase is the establishment of effective communications between the Finder and Vendor. The Finder contacts the Vendor via a published interface and provides the VSR. The Vendor acknowledges receipt of the VSR and optionally notifies the general public that it has an investigation underway.

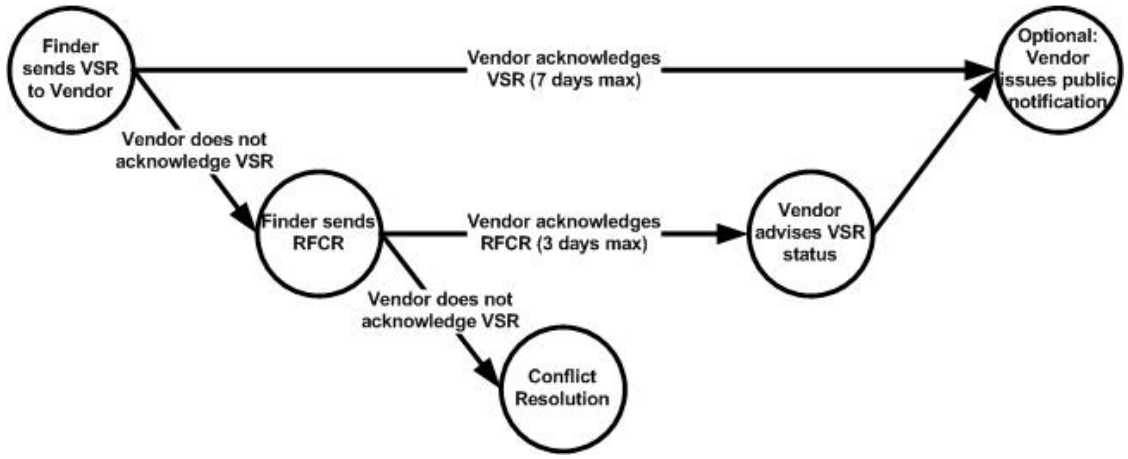

Figure 3. Steps in Notification Phase

5.1 Contacting the Vendor

The single most important element of a successful security response process is open and effective communications between the Finder and Vendor. This starts with the Vendor providing an easily discoverable point of contact through which potential security vulnerabilities affecting any of its products can be reported to it. By convention, this point of contact information should be discoverable via http://[vendor_domain]/security.

A variety of communication methods, including telephone and web forms, are successfully used throughout the industry; however, e-mail is most commonly used. E-mail addresses that are typically used for such purposes include:

- Security@[vendor_domain]
- Secure@[vendor_domain]
- Security-alert@[vendor_domain]
- Secalert@[vendor_domain]

Requirements

5.1.1 The Vendor shall provide a single person or organization to which all vulnerability reports involving its products can be sent.

5.1.2 The Vendor shall make reasonable efforts to accommodate Finders who wish to anonymously report vulnerabilities.

5.1.3 The Vendor shall post information for contacting it to one or more publicly accessible locations. The Vendor's security response policy shall indicate where this information is posted, or provide the contact information itself.

5.1.4 The Vendor's posted contact information shall, at a minimum, include:

- A reference to the Vendor's posted security response policy.
- A listing of the contact methods the Vendor supports.
- Contact instructions for each of the methods listed above.
- Instructions for using the secured communication channel discussed in paragraph 5.1.8 below, along with any needed cryptographic key material.

5.1.5 The Vendor shall exercise reasonable efforts to ensure that misdirected mails to the following email addresses can be re-routed to the appropriate point of contact:

- abuse@[vendor_domain]
- postmaster@[vendor_domain]
- sales@[vendor_domain]
- info@[vendor_domain]
- support@[vendor_domain]

5.1.6 The Finder shall alert the Vendor to the Potential Flaw by submitting a Vulnerability Summary Report (VSR), as discussed in Section 4.1 above ("Vulnerability Summary Report"), to one of the points of contact listed in paragraph 5.1.4 above.

5.1.7 If the Finder cannot identify the appropriate point of contact for the Vendor, it shall send an email to one or more of the alternate contacts listed in paragraph 5.1.5 above.

5.1.8 The Vendor shall provide a means of securing the communication channel between it and the Finder. Examples of frequently used methods include encrypted email or secured web sites.

5.1.9 The Vendor shall not make its cooperation with the Finder contingent upon the Finder's use of the secured communication channel discussed in paragraph 5.1.8 above.

5.1.10 If the Finder encrypts its communications using one of the methods discussed in paragraph 5.1.8 above, the Vendor shall reciprocate.

5.2 Acknowledgment of VSR

It is critical that the Vendor promptly acknowledge receiving the VSR. This confirms for the Finder that the Vendor is engaged, and provides a basis for establishing communications between the parties.

Requirements

5.2.1 If the Finder provides contact information, the Vendor shall acknowledge[4] receipt of the VSR upon receipt.

5.2.2 The Vendor's acknowledgment shall include a reference to the Vendor's Security Response policy, and may include a unique identifier for the investigation.

5.2.3 If the Finder does not receive acknowledgment within seven (7) calendar days of sending the VSR, the Finder may send a Request for Confirmation of Receipt[5] (RFCR).

5.2.4 The RFCR shall include a copy of the original VSR.

5.2.5 Upon receiving an RFCR, the Vendor shall acknowledge[6] its receipt, and shall advise the Finder of the status of the original VSR.

5.2.6 If the Finder does not receive acknowledgment within three (3) calendar days of sending the RFCR, the Finder may take the steps described in Section 3 above ("Conflict Resolution and Third Parties").

5.3 Public Notification of VSR

In some cases, the Vendor may wish to notify the general public that it has received a vulnerability report and is investigating it. If this is done, however, the Vendor should exercise care to avoid disclosing data that could put users and systems at risk.

Requirements

5.3.1 The Vendor may notify the general public that it has received a VSR and has an investigation underway.

5.3.2 The Vendor shall advise the Finder prior to issuing a public notification. This may be done through direct communications or documentation in the Vendor's security response policy.

5.3.3 If the Vendor chooses to issue a public notification, it shall it shall do so in accordance with the stipulations specified in Section 8 below ("Release Phase") and exercise reasonable efforts to make the notification available to all users who might be affected.

5.3.4 The Vendor shall only identify the Finder in the public notification with the Finder's advance approval.

6 Investigation Phase

Objective: The Vendor investigates the Finder's Vulnerability Summary Report in an attempt to verify and validate the Finder's claims, and works collaboratively with the Finder as it does so.

During Investigation Phase, the Vendor, in consultation with the Finder, conducts a thorough investigation that not only considers the specific claims in the VSR, but also goes beyond it to examine other related problems and additional products and versions. Throughout the investigation, the Vendor consults with the Finder as needed and provides status reports at agreed-upon intervals. At the conclusion of the investigation, the Vendor provides the Finder with its findings and substantiation.

[4] A sample acknowledgment is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

[5] A sample RFCR is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

[6] A sample acknowledgment is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

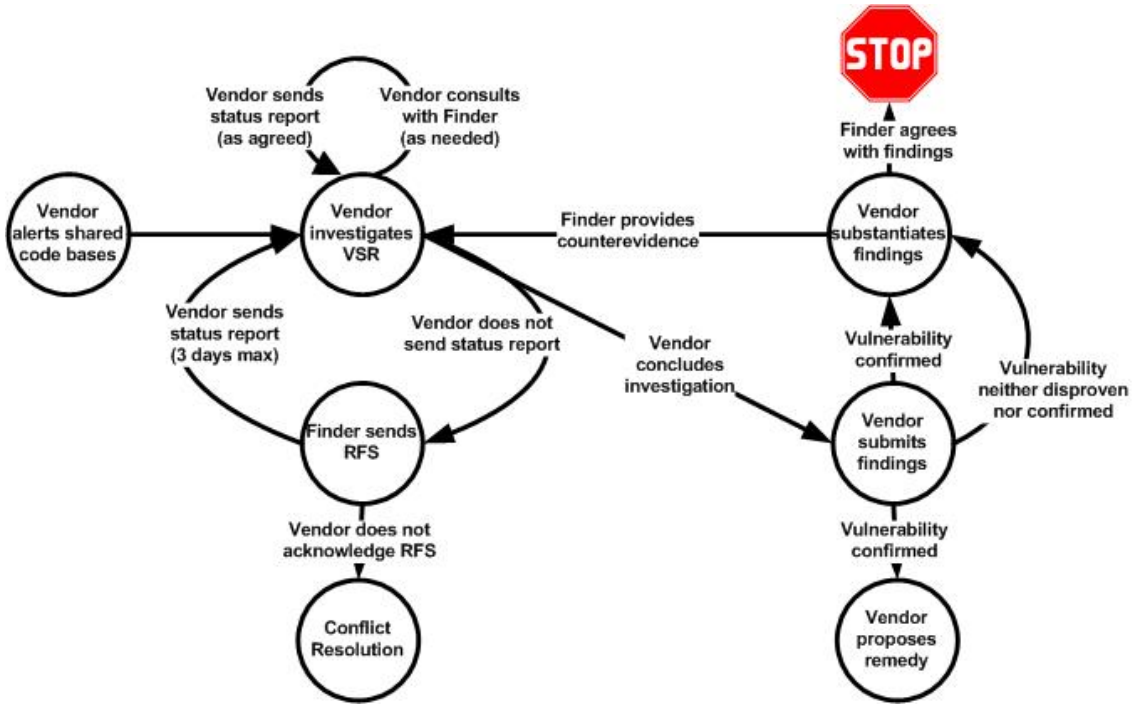

Figure 4. Steps in Investigation Phase

6.1 Status Updates

Regular status updates not only show the investigation's progress, but also provide the Finder with opportunities to offer feedback. By default, the Vendor should send status updates weekly.

Requirements

6.1.1 Unless otherwise agreed upon, the Vendor shall provide status updates[7] to the Finder no less often than every seven (7) calendar days.

6.1.2 The Vendor may use any mutually agreed-upon method of providing status updates. Examples of commonly used methods include:

- Telephone contact.
- E-mail.
- A secure repository, such as a secure web site or FTP site.

6.1.3 If the Vendor fails to provide status every seven (7) calendar days or at the agreed-upon interval (if different), the Finder may send a Request for Status[8] (RFS).

6.1.4 The RFS shall provide information showing that seven (7) calendar days or the agreed upon interval has passed since the last update.

6.1.5 Upon receiving an RFS, the Vendor shall acknowledge[9] receipt of the RFS and provide a status update.

6.1.6 If the Finder does not receive acknowledgment within three (3) calendar days of sending the RFS, the Finder may take the steps described in Section 3 above ("Conflict Resolution and Third Parties").

---

[7] A sample status report is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

[8] A sample RFS is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

[9] A sample acknowledgment is available from the OIS web site (http://www.oisafety.org/guidelines/samples).

6.2 Scope of Investigation

The Vendor should not limit its investigation to just the Finder's VSR, but instead should investigate additional supported products and versions, additional attack vectors, and so forth. The Vendor must investigate all currently supported products and may also investigate unsupported ones at its discretion. (This might be appropriate in cases where an expired product still has a large user base). However, the steps for investigating and remedying flaws in unsupported products is beyond the scope of these guidelines.

Requirements

6.2.1 The Vendor shall investigate whether the Potential Flaw exists in the supported versions of the product(s) discussed in the VSR.

6.2.2 The Vendor shall exercise reasonable efforts to determine whether the Potential Flaw exists in any supported products that were **not** discussed in the VSR.

6.2.3 The Vendor shall exercise reasonable efforts to identify and investigate attack vectors for the Potential Flaw in addition to those discussed in the VSR.

6.2.4 The Vendor shall maintain a public listing indicating which of its products, and which versions of those products, are supported.

6.3 Shared Code Bases

Security vulnerabilities sometimes affect products that, although maintained by different vendors, are based on the same source code. Coordinating a security investigation in such cases is complex, and the detailed processes for doing so are beyond the scope of this document. (They may be the subject of a future best practices document.) Broadly, though, the goals are to notify the other affected vendors, establish effective communications among them, and negotiate a coordinated plan for investigating the report and delivering remedies.

Requirements

6.3.1 If the Vendor or Finder finds that the Potential Flaw affects multiple vendors' products, it shall take at least one of the following actions:

- Exercise reasonable efforts to notify each Vendor.
- Contact an organization responsible for coordinating the efforts of the affected Vendors, if one exists.
- Enlist a Coordinator to assist in marshalling an effective response.

6.3.2 If the Vendor or Finder finds that the Potential Flaw affects multiple vendors' products, it shall take at least one of the following actions:

- Exercise reasonable efforts to notify each Vendor.
- Contact an organization responsible for coordinating the efforts of the affected Vendors, if one exists.
- Enlist a Coordinator to assist in marshalling an effective response.

6.3.3 The Vendor shall exercise reasonable efforts to establish and maintain communications with all vendors identified in paragraph 6.3.1 above.

6.3.4 The Vendor shall negotiate with the other affected vendors to develop a coordinated plan for investigating the Potential Flaw and taking appropriate steps.

6.3.5 The coordinated plan shall include, but not be limited to, the following:

- Communication processes
- Frequency and content of status updates.

6.4 Consultations During the Investigation

During the course of the investigation, the Vendor may consult with the Finder to request additional information. The Finder is not obligated to participate in these consultations, although it should be recognized that the investigation may be impeded or delayed without them.

Requirements

6.4.1 While the investigation is underway, the Vendor may request additional information from the Finder to assist in the investigation. Examples of such information include:
- Observed characteristics of the Potential Flaw.
- The environment in which the Potential Flaw occurs, including network and system configuration details.
- The involvement of any third party software in the Potential Flaw.

6.4.2 The Finder shall not be required to provide information beyond that in the VSR.

6.4.3 The Finder may provide any information that will assist the Vendor's investigation, including code that demonstrates the Potential Flaw.

6.5 Findings

At the conclusion of its investigation, the Vendor must report its findings to the Finder – either that it has confirmed the Flaw, disproved it, or is unable to do either – and must substantiate its findings. While the Vendor need not provide specific test procedures and results, the vendor has an obligation to show that it thoroughly investigated the report.

Requirements

6.5.1 The Vendor shall demonstrate that its investigation was thorough and technically sound, by providing the Finder with information such as:
- The list of products and versions it tested.
- The tests it performed.
- The outcome of the tests.

6.5.2 The Vendor shall report one of the following outcomes to the Finder:
- It has confirmed the Flaw.
- It has disproved the Potential Flaw.
- It can neither confirm nor disprove the Potential Flaw.

6.5.3 If the Vendor's investigation confirms the Flaw, it shall advise the Finder of its plans for addressing the issue. Specifically, the Vendor shall provide the following information:
- The supported products and versions affected by the Flaw.
- The Vendor's proposed vehicle for distributing the remedy (see Section 7.3 below, "Remedy Types").
- The Vendor's proposed timetable for releasing the remedy.

6.5.4 In order to report disproof of the Potential Flaw, the Vendor shall show that either or both of the following conditions are true:
- The Potential Flaw does not exist in any supported product.
- The behavior the Finder reported does exist, but does not constitute a security vulnerability.

6.5.5 If the Vendor confirms the behavior the Finder reported, but concludes that it does not constitute a security vulnerability, it shall substantiate its judgment by providing data such as:
- Product documentation confirming that the behavior is by-design and explaining why it is reasonable.

- Test results showing that the behavior only occurs when the product is configured in a way that itself violates normal security practices and exposes the system to significant risk.
- Analysis of the attack scenario, showing that the behavior could not be realistically exploited or could only be exploited in cases where the system was already insecure.

6.5.6 If the Vendor is unable to either confirm or disprove the Potential Flaw, the Vendor shall advise the Finder of the testing it has performed, the results it has witnessed, and the evidence it would require to either confirm or disprove the report.

6.5.7 If the Finder disputes the Vendor's findings, it shall provide substantiation such as:

- Test results that contradict the Vendor's findings.
- Analysis of the attack scenario, showing that the behavior could be exploited realistically and in cases where the system was otherwise secure.

6.5.8 A disputing Finder may provide any information that will assist the Vendor in resolving the dispute, up to and including code that demonstrates the Potential Flaw.

6.5.9 A disputing Finder shall not be required to provide information to conclusively resolve a dispute.

6.5.10 The Vendor shall investigate any additional data or analysis provided by a disputing Finder, and update its findings as appropriate.

6.5.11 Regardless of the Vendor's findings, the Finder may publish information concerning the Potential Flaw.

6.5.12 If the Finder chooses to publish information concerning the Potential Flaw per paragraph 6.5.11 above, it shall do so in accordance with the stipulations specified in Section 8 below ("Release Phase").

7 Resolution Phase

Objective: If the Potential Flaw is confirmed, the Vendor identifies where the Flaw resides, then develops a remedy that eliminates or reduces the risk of the vulnerability.

Resolution Phase presupposes the case where a vulnerability has been confirmed. During this phase, the Vendor, working in concert with the Finder, determines the appropriate remedy for the vulnerability, implements it, and takes steps to ensure that it is thoroughly tested and eliminates the vulnerability.

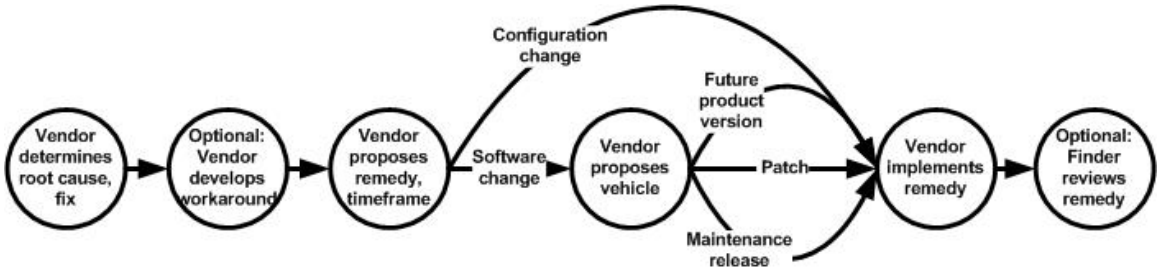

Figure 5. Steps in Resolution Phase

7.1 Remedy

If the investigation confirms that a vulnerability does exist, the Vendor develops a remedy for all supported products and versions. In many cases, the Vendor will provide root-cause data, preliminary versions of the remedy, or other data to the Finder, and seek the Finder's assistance in corroborating its findings or confirming the quality of the remedy. Although this is optional for

both parties – the Vendor is not required to supply such data, nor is the Finder obligated to assess it – doing so can significantly contribute to the quality of the solution.

Requirements

7.1.1 Upon confirming that the Flaw exists, the Vendor shall determine whether a remedy for it is already available.
7.1.2 If a remedy for the Flaw already exists, the Vendor shall notify the Finder of its availability.
7.1.3 If a remedy for the Flaw does not exist, the Vendor shall develop one.
7.1.4 The Vendor shall ensure that a remedy is available for all supported products affected by the Flaw.
7.1.5 The Vendor may share any desired data, in any level of detail, with the Finder, in order to enable them to confirm the quality of the investigation and remedy.
7.1.6 The Finder shall not be obligated to take any action in response to data provided to it per paragraph 7.1.5 above.
7.1.7 The Vendor shall take reasonable efforts to ensure that the Flaw is not included in any future versions of the product.

7.2 Timeframe

An effective security response process minimizes the risk posed by security vulnerabilities to customers, critical infrastructures, and the Internet. Speed is an essential element of such a process, but is by no means the only factor. Equally important is the thoroughness of the investigation, the quality of the fix, and the measures taken to ensure high uptake of the fix.

The best response balances all of these factors to provide the most effective risk reduction possible. The appropriate timeframe will vary from case to case, but it is important to set a target. By convention, thirty (30) calendar days (measured from the date the Vendor acknowledges receipt of the VSR to delivery of the fix) has been established as a good starting point for the discussions, as it often provides an appropriate balance between timeliness and thoroughness.

Requirements

7.2.1 The Vendor shall propose an appropriate timeframe for resolving the vulnerability.
7.2.2 The Vendor shall substantiate its proposal by reference to relevant factors such as:
- The risk the vulnerability poses.
- The engineering complexity of the remedy.
- The degree of testing required.
- The steps needed to ensure high uptake of the fix.

7.2.3 If the Finder believes that a significantly longer or shorter timeframe than that proposed by the Vendor is appropriate, it shall substantiate its position by reference to relevant criteria such as those listed in paragraph 7.2.2 above.

7.3 Remedy Types

Two types of remedies are typically available for security vulnerabilities: configuration changes or software changes. Configuration changes involve changes in the way users operate the product, and typically are implemented by either modifying the product's operating parameters or by using an alternative usage scenario.

Software changes involve changes in the implementation of the product, and typically are effected via any of three vehicles:

- **Patches**. These are unscheduled special releases that address a small number of fixes.

- **Maintenance Updates**. These are scheduled releases that address a large number of fixes. (Some vendors refer to these updates as service packs, service releases, or maintenance releases).
- **Future product versions**. These are major, scheduled product revisions, typically encompassing design and feature changes.

The appropriate type of fix depends, in large part, on the risk the Flaw poses, the engineering difficulty of the fix, and the availability of the various vehicles. For instance, if a maintenance update were due to be released imminently, it might be appropriate to use it as the vehicle for fixing a particular security vulnerability. In contrast, if the maintenance update were many months from release, the same vulnerability might warrant a patch or a configuration change.

Likewise, it may be appropriate to deliver fixes of different types for the same vulnerability. For instance, if Product 1 and Product 2 were affected by the same vulnerability, it might, depending on the circumstances, be appropriate for the Vendor to include the fix for Product 1 in the maintenance update and deliver the fix for Product 2 via a configuration change.

Requirements

7.3.1 Upon completing its investigation, the Vendor shall propose a remedy that, in its judgment, represents a reasonable means of protecting users, the Internet, and critical infrastructures that depend on it.
7.3.2 The Vendor shall propose a remedy that takes the form of a configuration change, software change, or other appropriate action.
7.3.3 The Vendor shall advise the Finder of its proposed remedy and substantiate its proposal.
7.3.4 If the Finder disagrees with the Vendor's proposed type of remedy, it shall propose an alternative type of remedy and substantiate its proposal.
7.3.5 The Vendor may effect configuration changes via manual instructions, automated configuration tools, or other appropriate methods.
7.3.6 The Vendor may effect software changes via patches, maintenance updates, future product versions, or other appropriate methods.
7.3.7 The Vendor may, if appropriate, deliver different types of remedies for flaws affecting multiple products or versions.
7.3.8 The Vendor shall take reasonable efforts to ensure that side effects, compatibility problems, and other limitations associated with the remedy are investigated and clearly documented.

7.4 Simultaneity

Security vulnerabilities sometimes affect multiple versions of a product or multiple products. The Vendor's goal in such cases should be to simultaneously deliver the remedies for all instances of the vulnerability. However, this is not always possible. In some cases, the different instances of the vulnerability have significantly different engineering complexity, testing requirements, and so forth, resulting in different completion dates for the remedies.

A dilemma arises regarding the delivery strategy when remedies have significantly different completion dates. Delivering them piecemeal minimizes the risk to some systems, but exposes the fact that other systems cannot yet be protected. In contrast, delaying their release until all are completed leaves all affected systems equally exposed until the final remedy is available. Neither of these alternatives is desirable, and this section discusses a strategy for handling such cases.

Requirements

7.4.1 If multiple products or versions are affected by the Flaw, the Vendor shall exercise reasonable efforts to simultaneously deliver all remedies.

7.4.2 If, for reasons of engineering complexity or other factors, the remedies for different products or versions cannot be completed simultaneously, the Vendor may release them non-simultaneously.

7.4.3 If the Vendor chooses a non-simultaneous release, it shall prioritize the remedies according to risk, and exercise reasonable efforts to provide interim measures (see Section 7.7 below, "Workarounds") for protecting systems that do not yet have a remedy available.

7.5 Internationalization

Many vendors' products are available in multiple languages. It is critical that remedies be available for all supported languages, delivered simultaneously when possible.

Requirements

7.5.1 If the affected products are available in multiple languages, the Vendor shall ensure that a remedy is delivered for each of the supported languages.

7.5.2 The Vendor shall exercise reasonable efforts to deliver the remedies for all supported languages simultaneously.

7.5.3 If the Vendor chooses, because of engineering complexity or other reasons, to release the remedies non-simultaneously, it shall prioritize them according to user base size.

7.6 Synchronization

As discussed in Section 6.3 above ("Shared Code Bases"), the specific processes for synchronizing a security investigation involving multiple vendors is beyond the scope of this document. However, as a general guideline the vendors should minimize the risk posed to all vendors' customers by negotiating a coordinated release plan for their respective remedies and taking reasonable efforts to adhere to it.

Requirements

7.6.1 If a Flaw affects multiple vendors' products, the Vendor shall negotiate with other affected vendors to establish a target date for releasing all vendors' remedies.

7.6.2 The Vendor shall not be required to agree to a coordinated plan if doing so would, in its judgment, conflict with protecting users, the Internet, and the critical infrastructures that depend on it.

7.6.3 If the Vendor chooses to release its remedy independently, it shall inform the Finder and all coordinating Vendors of its decision, and shall exercise reasonable efforts to provide ample lead time before doing so.

7.6.4 If the Vendor chooses to release its remedy independently, it shall limit the information it publishes about the vulnerability, in order to avoid putting at risk other users who may not have a remedy available.

7.7 Workarounds

In some cases, it may be appropriate for the Vendor and/or Finder to release an interim protective measure while the remedy is being developed. Such workarounds typically involve temporarily changing the configuration of the product or network environment in which it operates. Because the uptake rate for workarounds is low, they should only be used in unusual cases; for example, if the timeframe for delivering the remedy to a particularly high-risk vulnerability will be especially long, or a high-risk vulnerability is already under active exploitation.

Requirements

7.7.1 The Finder or Vendor may propose publishing a workaround as an interim measure while the remedy discussed in Section 7.3 above ("Remedy Types") is being completed.

7.7.2 The party proposing the workaround shall substantiate its proposal by reference to factors such as:

- The number of systems at risk and the imminence of the risk.
- The timeframe for a remedy.
- The disruption that the proposed workaround will entail.
- The workaround's likely uptake.

7.7.3 Publishing a workaround shall require the mutual consent of both parties.

7.7.4 If the Finder and Vendor agree to publish a workaround, both shall exercise reasonable efforts to avoid disclosing details that would aid attackers in exploiting the vulnerability.

8 Release Phase

Objective: In a coordinated fashion, the Vendor and the Finder publicly release information about the vulnerability and remedy.

In Release Phase, the Vendor and Finder develop documentation thoroughly describing the vulnerability, the risk it poses, and steps users can take to minimize or eliminate it. When the remedy is complete the Vendor releases it, following which the Vendor and Finder release their respective documentation in concert. In the interest of providing users with a reasonable period during which to defend their systems, the parties delay the public release of data that could directly lead to the vulnerability being exploited.

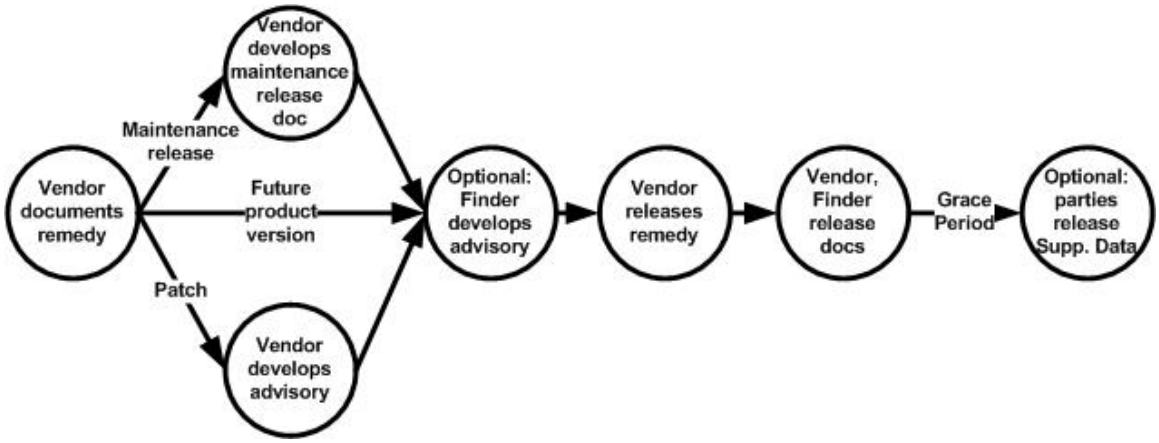

Figure 6. Steps in Release Phase

8.1 Advance Notification

This document does not address processes for notifying selected groups of users about vulnerabilities in advance of the general population. While such "pre-release notifications" are sometimes done, and in very well-controlled cases can be carried out effectively, they are not a recommended practice in the general case. To cite just two examples of why this is so, there is no industry-wide consensus regarding the selection criteria for advance notification; and such data, if leaked, could increase the risk to the general population. Because this document addresses only activities that are appropriate for typical cases, advance notification is beyond its scope.

8.2 Documentation

The appropriate type of documentation to accompany a remedy depends on the specific delivery vehicle for the fix. In addition, as discussed below, it may be appropriate in some cases to provide supplementary data regarding a vulnerability to selected audiences.

Requirements

8.2.1 If the Vendor's remedy takes the form of a patch or configuration change, the Vendor shall provide a Security Advisory, as detailed in Section 8.3 below ("Security Advisory").

8.2.2 If the Vendor's remedy takes the form of a maintenance update, the Vendor shall discuss the fix as part of the maintenance update documentation.

8.2.3 The Vendor shall not be required to list changes that were made as part of a new product or version.

8.3 Security Advisory

The purpose of a security advisory is to provide information that assists the general public in understanding a security vulnerability, the products and versions it affects, and the steps that can be taken to defend affected systems and networks against it.

Requirements

8.3.1 The Vendor shall provide a single repository for all security advisories regarding its products.

8.3.2 The Vendor's Security Response Policy shall list the location of the repository.

8.3.3 The Vendor shall make the repository accessible to the general public, and easily discoverable.

8.3.4 The Finder may provide a repository for the security advisories it publishes. If so, the Finder's Security Reporting Policy shall list the location of the repository.

8.3.5 The Finder and Vendor shall provide a means by which readers can confirm the authenticity and origin of their security advisories. Examples of commonly used methods include digitally signing it or hosting it on an SSL-protected web site.

8.3.6 The Vendor may provide a means of proactively notifying interested parties when new security advisories are published. Examples of such a system include subscription mail services and automated pager alerts.

8.3.7 The Finder may publish its security advisories on its own subscription mail lists or public vulnerability disclosure lists.

8.3.8 The Vendor and the Finder shall exercise reasonable efforts to release their security advisories simultaneously, and only after a remedy is available to the general public.

8.3.9 The Vendor and Finder shall provide information of a defensive nature in the security advisory, such as:

- Methods by which to identify affected systems.
- Information useful in evaluating the risk the vulnerability poses and the priority that should be assigned to addressing it.
- The types of fixes that are available, along with information that assists the user in selecting an appropriate one.

8.3.10 The Vendor and the Finder shall exercise reasonable efforts to avoid providing supplementary data in their security advisory, except pursuant to Section 8.6 below, "Supplementary Data").

8.3.11 The Vendor's and Finder's Security Advisory shall, at a minimum, contain the following information:

- Advisory Name: A unique descriptive name or title that identifies the advisory.
- Release Date: The publication date of the Security Advisory.
- Product: The product(s) and version(s) the vulnerability affects.

- Platform: The operating system(s) the vulnerability affects.
- Effect: A short description of the effect of a successful attack .
- Vulnerability Identifier: A unique identifier for the vulnerability[10], if available.
- Details: A detailed presentation of information such as: how the vulnerability manifests itself; the affected components and configurations; mitigating factors; workarounds; steps to guard against similar problems if they exist.
- Recommendations: A discussion of options for eliminating or mitigating the vulnerability, such as: vendor patch information, configuration changes, additional software or hardware protection methods, and methods for detecting vulnerable systems.
- Caveats: Any known side effects or limitations associated with the fix.
- Signature Information: a link to the key used to sign the Security Advisory, if any. (See paragraph 8.3.5 above).

8.3.12 The Vendor's and Finder's Security Advisory may contain additional information, such as the following:

- Overview: An executive summary of the vulnerability and remedy.
- Root Cause: The underlying flaw that causes the vulnerability.
- Attack Vectors: The scenario(s) via which an attacker could exploit the vulnerability, subject to paragraph 8.3.10 above.
- Vulnerability Identifier Cross-Reference: A consolidated listing of all identifiers assigned to the vulnerability, and the systems that assigned them.
- Timeline: The dates of important milestones in the security response process, such as the date the VSR was submitted, the date on which the Vendor reported its finding to the Finder, and so forth.
- Acknowledgment: A reference to participants' contribution to the investigation, subject to their desire for such acknowledgment. Advisory publishers may establish criteria for qualifying for acknowledgment in the organization's security policy.
- Security Policy: A reference to the publisher's security response policy.

8.3.13 The Finder's Security Advisory shall provide a link to the Vendor's security bulletin to ensure that readers can obtain the remedy.

8.4 Independent Release of Security Advisory

As discussed in paragraph 8.3.8 above, the Finder and Vendor should act in concert to simultaneously release their advisories after a remedy is available. However, if a third party publicly discloses the vulnerability before the remedy's release date, or if the vulnerability comes under active exploitation, it may be necessary to act separately. Even in this case, however, it is important to avoid exacerbating an already bad situation.

Requirements

8.4.1 If a third party publicly discloses the vulnerability before the release date agreed to by the Finder and Vendor, or if the vulnerability comes under active exploitation, both may independently release their security advisories.

8.4.2 Before independently releasing its advisory, the Finder or Vendor shall exercise reasonable efforts to alert the other party.

8.4.3 Before independently releasing its advisory, the Finder or Vendor shall share evidence with the other party substantiating that one or more of the prerequisites have been fulfilled.

[10] The Common Vulnerabilities and Exposures program (http://www.cve.mitre.org/) is the most commonly used vulnerability identification system

8.5 Maintenance Update Documentation

The overall content and format of maintenance update documentation is beyond the scope of these guidelines. However, when a maintenance update is used as the vehicle for delivering a fix for a security vulnerability, it is important to provide information that enables customers to evaluate the priority of installing it.

Requirements

8.5.1 If the Vendor chooses a maintenance update as the delivery vehicle for a remedy to a security vulnerability, the Vendor shall clearly indicate this by including information such as:

- The effect of exploiting the vulnerability.
- Configuration settings that make a system more or less susceptible to attack via the vulnerability.
- Known side effects of the remedy.

8.6 Supplementary Data

As discussed in Section 8.3 above ("Security Advisory"), the Vendor and Finder should publish a broad array of data to assist the general public in identifying and defending vulnerable systems. However, in the course of the investigation, the Vendor and Finder may also develop additional, more sensitive data, which this document terms *supplementary data*.

Supplementary data is defined here as data that directly provides the means of exploiting the vulnerability. The use of the word "directly" is critical to the definition. Other data – even if, through analysis, it could be used to develop a means of exploiting the vulnerability – does not meet this definition. Thus, exploit tools and step-by-step instructions would constitute supplementary data, but the source code of a fix or root-cause details would not.

Supplementary data can aid security in certain cases, such as in the case of an intrusion detection or anti-virus vendor that uses it to develop countermeasures to the vulnerability. Likewise, it can aid academic and other organizations' research into needed engineering quality improvements. However, it can also undermine security by assisting malicious users in learning how to exploit the vulnerability. This section describes a compromise that attempts to balance these competing interests.

During the first thirty (30) calendar days after the release of the fix, the Vendor and Finder restrict the release of supplementary data in the interest of giving users time to protect their systems, and share it only with people or organizations associated with defending systems against the vulnerability, protecting critical infrastructures, law enforcement, and so forth. Once this grace period expires, the supplementary data can be distributed as each party deems .

Requirements

8.6.1 The Finder and Vendor shall observe a grace period that shall start with the release of the fix and last for thirty (30) calendar days.

8.6.2 The grace period shall immediately expire if the same supplementary data is publicly released by another party, or if the vulnerability becomes actively exploited.

8.6.3 During the grace period, the Vendor or Finder shall share supplementary data only with people or organizations that are directly involved in providing tactical response to the vulnerability or protecting critical infrastructures, and only after exercising reasonable efforts to ensure that an effective legal or other framework is in place to prevent the uncontrolled onward dissemination of the information.

8.6.4 At the expiration of the grace period, the Vendor and Finder may distribute supplementary data at its own option and risk, with people or groups of its choice.

8.6.5 If the Finder or Vendor declares the grace period expired pursuant to paragraph 8.6.2 above, it shall share evidence with the other party substantiating that one or more of the prerequisites have been fulfilled.

8.6.6 These restrictions shall not apply to sharing data with law enforcement authorities, or sharing it in compliance with local laws.

Legal Information

The information contained herein is not a license, either expressly or impliedly, to any intellectual property owned or controlled by any of the authors or developers of this standard. The information contained herein is provided on an "AS IS" basis and to the maximum extent permitted by applicable law, this information is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this standard hereby disclaim all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the contribution.

ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE STANDARD.

IN NO EVENT WILL ANY AUTHOR OR DEVELOPER OF THIS STANDARD BE LIABLE TO ANY OTHER PARTY FOR THE COST OF PROCURING SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, OR PUNITIVE OR SPECIAL DAMAGES WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, ARISING IN ANY WAY OUT OF THIS OR ANY OTHER AGREEMENT RELATING TO THIS DOCUMENT, WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGE.