



Symantec Responsible Disclosure Policy

Symantec Consulting Services Advisory Coordination Team
January 2006

Purpose

Process

Policy

Suggestions for vendors

Suggestions for customers

Copyright © 2006 by Symantec Corporation. All rights reserved.

With the exception of redistribution electronically in its entirety through authorized means, this document may not be copied or redistributed in any manner. This document may not be modified, edited or amended except by Symantec Corporation. Reprinting the whole or parts of this document in any medium other than electronically, requires permission from Symantec Corporation. Requests may be sent to cs_advisories@symantec.com.

Disclaimer

Symantec makes this document available for informational purposes only. While Symantec believes that the information in this document is accurate at the time of publishing based on currently available information, it may not reflect the most current legal and business developments, and Symantec does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. This document makes no representations or warranties of any kind and is not intended to constitute legal advice. Readers should not act (or refrain from acting) based on the information herein without obtaining professional advice regarding your particular facts and circumstances. Opinions presented in this document reflect judgment at the time of publication and are subject to change. While every precaution has been taken in the preparation of this document, the information is provided “as is” and Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein.

Symantec, Symantec products, and SymSecurity are registered trademarks of Symantec Corporation and/or affiliated companies in the United States and other countries. All other registered and unregistered trademarks represented in this document are the sole property of their respective companies/owners.

Table of Contents

PURPOSE	4
SCOPE	4
PROCESS OF VULNERABILITY REPORTING	4
POLICY	5
Phase 1: Discovery	5
Phase 2: Notification and Acknowledgement.....	5
Phase 3: Validation.....	6
Phase 4: Resolution	7
Phase 5: Release	8
SUGGESTIONS FOR VENDORS	9
SUGGESTIONS FOR CUSTOMERS	10
VULNERABILITIES VERSUS EXPOSURES	11
REFERENCES	11

PURPOSE

For computer industry vendors, our customers, and the public, this policy outlines how Symantec Corporation (“Symantec” hereafter) manages the public reporting of security vulnerability information it has concerning products developed by other organizations/owners/vendors/developers (“vendor” hereafter). This policy intends to enable all parties to understand and address vulnerabilities expeditiously in their environment and to minimize the risks that the vulnerability information poses.

The goals of the policy are:

- To assist in the identification and remediation of vulnerabilities in a manner which is effective and efficient for all parties.
- To minimize the risk to all parties from such vulnerabilities.
- To provide all parties with information that supports independent corroboration of these vulnerabilities.
- To provide the security community with the information necessary to learn from these vulnerabilities and thus identify, manage, and reduce the risks of future vulnerabilities in information technology.
- To minimize the amount of time and resources that all parties would otherwise be required to use in managing these vulnerabilities.
- To facilitate long-term research and development of techniques, products, and processes for understanding, avoiding, or mitigating security vulnerabilities.
- To circumvent such antagonism as can sometimes arise in the absence of a formal disclosure policy such as this one.

SCOPE

Security vulnerabilities and exposures can and do occur as the result of flaws in hardware products, network architectures, operational procedures, and other factors. While it is important to identify and remedy security vulnerabilities and exposures that result from such factors, the technical process by which this should be done is beyond the scope of this document.

PROCESS OF VULNERABILITY REPORTING

The basic steps of the Symantec Security Vulnerability Reporting Process, with details in the subsequent section of this document, are below. These steps are aspirational in nature, and while Symantec will attempt to follow them and encourages the other parties involved to follow them, there can be no guarantees that differing factual situations will not affect any parties' implementation of the process.

By providing this information to the vendor, Symantec is in no way obligated to take any action to fix or mitigate the vulnerability in any way. The vulnerability information Symantec provides is supplied as a courtesy to the vendor, and to enhance the security of the Internet community as a whole. Symantec makes no warranties with respect to the

information provided herein or pursuant to this policy and accepts no responsibility for any actions or inactions taken as a result of the use of, or reliance on, this information.

1. **Discovery.** Symantec discovers a security vulnerability ("The Flaw") either by accident or while working on specific security research.
2. **Notification.** Symantec notifies the vendor of the product that contains the Flaw ("Initial Full Notification"). In turn, the vendor provides Symantec with evidence that the Initial Full Notification was received ("Vendor Receipt").
3. **Validation.** The vendor tries to verify and validate Symantec claims ("Reproduction").
4. **Resolution.** The vendor tries to identify where the Flaw resides ("Diagnosis"). The vendor develops a patch or workaround that eliminates or reduces the risk of the vulnerability ("Fix Development"). The Fix Development is then optionally tested by Symantec to ensure that the Flaw has been corrected ("Patch Testing"). Symantec notifies the vendor of the outcome of the Patch Testing.
5. **Release.** In a coordinated fashion, the vendor and Symantec publicly release information about the vulnerability, along with its resolution ("Security Advisory").

POLICY

The following describes how Symantec intends to operate during each phase of the Security Vulnerability Reporting Process.

Phase 1: Discovery

Symantec will validate its findings and draft a written Vulnerability Summary Report (VSR). The written report will include succinct examples to enable the vendor to quickly assess the potential flaw. The VSR will include:

- A text-only advisory describing the issue, including affected platforms and versions
- A detailed technical description including step-by-step instructions for reproducing the issue
- If available, 'proof of concept' code to aid in diagnosis by the vendor

Phase 2: Notification and Acknowledgement

If Symantec is not able to identify the appropriate security-related email address for that vendor, an email will be sent to one or more of the following contacts if available from the vendor's Web site:

- the official domain contacts for the vendor
- security@
- secure@
- security-alert@

- secalert@
- support@
- info@
- sales@

The initial contact email from Symantec will inform the vendor that a security vulnerability has been found in one or more of the vendor's products. Since the premature release of detailed technical information regarding an unresolved vulnerability can be dangerous, no details will be included in the initial contact email. To ensure confidentiality, integrity, and authenticity for all subsequent information exchanges between Symantec and the vendor, Symantec will provide a PGP (Pretty Good Privacy) key in this initial contact email and request a vendor PGP key before sending the full Vulnerability Summary Report. The initial email sent to the vendor will also reference this document (<http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf>).

Upon receipt of the vendor's PGP key or a suitable secure communication alternative, Symantec will send an encrypted and signed email containing the VSR to the vendor, describing the vulnerability in detail. Symantec will record this full notification date.

Once the full notification containing the VSR is sent by Symantec, Symantec will expect a response by email from the vendor within 7 days that (a) acknowledges that the vendor has received and read the Symantec VSR and (b) describes any plans to address what is described in the Symantec VSR.

Phase 3: Validation

During this phase, it is anticipated that the vendor will attempt to address the vulnerability. The following is a list of suggestions for vendors to ensure that the resolution is satisfactory for their customers. These suggestions are expressed as "should" consistent with Symantec's understanding of best practices at this time.

1. If the vulnerability is found in a supported product, the vendor should
 - a. reproduce the vulnerability
 - b. determine if there is enough evidence for the existence of the vulnerability if it cannot be reproduced
 - c. determine if the vulnerability is already known (and possibly already resolved)or
 - d. work with Symantec's or other security experts to determine if the vulnerability is related to the specific environment in which it was discovered (including configuration errors or interactions with other products). As resources permit, Symantec will help the vendor with the validation phase when requested.
2. If the vulnerability is found in an unsupported or discontinued product, the vendor may refuse to validate the vulnerability. However, the vendor should undertake measures to ensure that the reported vulnerability does not exist in supported product versions or other supported products based on the vulnerable product.

3. The vendor should examine its product to ensure that it is free of other problems that may be similar to the reported vulnerability. Related vulnerabilities in the same product are often found by others after a specific vulnerability is publicly disclosed. Finding multiple vulnerabilities up front during the validation phase saves the vendor and customers time and money by minimizing the need to create and install multiple patches.
4. The vendor should provide status updates to Symantec every 7 days. The vendor and Symantec may come to an agreement for sharing less frequent updates.
5. The vendor should notify Symantec when they are able to reproduce the vulnerability.
6. The vendor should attempt to resolve the vulnerability as described in phase 4 within 30 days of initial notification. There are valid reasons why vulnerabilities cannot be resolved within this time period. If a good faith effort is being made by the vendor to validate the vulnerability, Symantec will delay the public disclosure of information about the vulnerability until a resolution is found or created.
7. If the vendor is aware of other vendors that share the same codebase as the affected product, the vendor should either (1) notify those vendors, or (2) notify a vulnerability coordinator, such as CERT/CC, that other vendors may be affected by the reported vulnerability.

Phase 4: Resolution

The resolution of a vulnerability should involve action regarding one or more of the following:

- patch creation
- recommendation of configuration change
- design change
- workaround

During this phase, Symantec recommends that the vendor should:

1. Identify the fundamental nature of the flaw within the source code or in the design of the product ("Diagnosis").
2. Determine whether to (a) provide a patch, configuration change, or workaround that appropriately reduces or eliminates the risk of the vulnerability ("Fix Development"), or (b) provide Symantec with specific reasons for their decision to pursue an alternative to fixing the vulnerability.
3. Request time extensions from Symantec when necessary.
4. Test the patches, configuration changes, and workarounds sufficiently to clarify how it might or may not adversely affect the operation of the product.
5. Provide Symantec with all known configuration changes or workarounds that address the vulnerability ("Fix Development"). The vendor should also provide Symantec with any patches so we may optionally conduct our own testing of the fix ("Patch Testing"). This helps us confirm that the vulnerability has been reduced or eliminated. A vendor may have existing policies in place that require

that only supported customers have access to this information; these policies should also be communicated to Symantec by email.

If the vendor does not participate in the validation or resolution phases, or if the vendor is unresponsive to Symantec, we believe that it is unlikely that the vendor's customers will be fully satisfied.

Phase 5: Release

1. Symantec will work with the vendor to create a timetable pursuant to which the vulnerability information may be released to Symantec customers, the vendor's customers, and the general public in a coordinated fashion.
2. However, if the parties cannot agree to a coordinated release of the vulnerability information, Symantec will honor a "Grace Period" of up to 30 days, during which we will unilaterally release only summary information ("Advance Security Advisory") to the public. The Advance Security Advisory will not include details of the vulnerability in an effort to reduce the likelihood that attackers might exploit the product based on receiving the new vulnerability information. Symantec will take every effort to describe or publish workarounds, configuration changes, or even patches where this information is not available from the vendor. After the expiration of the 30-day grace period Symantec will publicly release the full Security Advisory.
3. If the vendor has not resolved the vulnerability within the timeframe determined in the Release Phase, then Symantec may work with a coordinator, such as CERT/CC (<http://www.cert.org>) to announce the vulnerability to customers and the public.
4. In the event that no acknowledgement is received by Symantec from the vendor, Symantec will continue to attempt to contact the vendor through all known email channels in order to communicate Symantec's advisory release schedule for the identified vulnerability. All contact attempts will be documented and included in the Symantec Security Advisory under the "Vendor Response" section.
5. If another reporter has publicly announced the vulnerability before the release date agreed to by Symantec and the vendor, Symantec may immediately share details of the vulnerability with its customers who might be exposed to the newly public vulnerability.
6. Symantec's public release ("Security Advisory") will contain the following information:
 - a. Advisory Name: a descriptive name
 - b. Release Date: the date the Security Advisory is released to the public
 - c. Product: the name of the vulnerable product(s) with the specific affected versions
 - d. Platform: the operating system(s) or other platform information
 - e. Severity: A one-line description of the severity such as "remote execution of code" or "local privilege escalation".
 - f. Author: the author or authors of the Security Advisory

- g. Vendor Status: information about the anticipated availability of a bulletin or patch from the vendor
 - h. CVE Candidate: CVE candidate vulnerability reference number (information regarding CVE is available at <http://cve.mitre.org>).
 - i. Reference: a URL to the security advisory within the vulnerability database archives on the SecurityFocus web site
 - j. Overview: an executive overview of the vulnerability.
 - k. Details: The details may contain some or all of the following: a description of how the vulnerability presents itself, components and configurations that are affected, mitigating factors, workarounds or configuration changes to resolve the vulnerability, and/or preventative measures for similar problems in the future.
 - l. Vendor Response: Symantec will include vendor information, if provided, such as a brief statement, a link to a security bulletin or patch information in our public release. This makes it easier for customers to find the information they need in order to address the vulnerability in their environment. In cases where the vendor remains unresponsive to Symantec's attempts to communicate the vulnerability, this section will enumerate all communication attempts.
 - m. Recommendations: Symantec will recommend available courses of action for customers to eliminate or mitigate the vulnerability in their environment. The customer must decide the course of action, if any, which is best for their environment. This section will include one or more of the following: vendor patch information, configuration changes, additional software or hardware protection methods, and methods for detecting and finding vulnerable systems.
 - n. Disclosure Policy: a link to this document.
 - o. Signature Information: a link to the key used to sign the Security Advisory on the Symantec Web site
7. The Security Advisory will not contain the following information:
- a. Proof of concept code or test code that could readily be turned into an exploit
 - b. Sufficiently detailed technical information, such as exact data inputs, buffer offsets, or shell code strategies that could expedite the writing of exploit code

SUGGESTIONS FOR VENDORS

Symantec provides the following recommendations solely as suggestions to vendors, on an "as is" basis without warranty or guarantee of any kind, in order to provide guidance on how vendors can address and remediate security issues in their products.

1. Vendors should provide a security contact address on their web site and make it easy to find.

2. Vendors should set up a security response process to respond to security issues in a timely manner.
3. Vendors should provide a secure mechanism, such as PGP, to ensure confidentiality, integrity, and authenticity of communication with vulnerability discoverers and advisory release coordinators.
4. Vendors should incorporate lessons learned into training for their security, IT, product and marketing organizations.
5. Vendors should notify customers that someone has reported a problem, present a temporary work-around and/or tell customers that they are working to provide a final resolution.
6. Vendors should clearly notify customers and the public when a resolution is (a) faulty, or (b) revised.
7. Vendors should credit the reporter who notified them of the vulnerability if the reporter was working to responsibly protect customers.
8. Vendors should create and communicate a vulnerability response policy which details how they respond to and assess reports of vulnerabilities, how long customers should expect to wait for a typical resolution, and information about vulnerability reporting standards, if any, that they follow.

SUGGESTIONS FOR CUSTOMERS

Symantec provides the following recommendations solely as suggestions to customers on an “as is” basis without warranty or guarantee of any kind, in order to provide guidance on how to interpret security vulnerability information on products the customer uses. It is up to the customer’s discretion whether or not to follow these suggestions.

The customer must not assume that the lack of details in a public vulnerability report will prevent the creation of an exploit.

1. If a vendor has released information regarding a vulnerability, then the customer should assume that the information is credible. The customer should not require that the vulnerability be demonstrated before applying the resolution.
2. If a vendor has not released such information, but a well-established reporter or coordination center has, then the customer should assume that the information is credible. The customer should not require that the vulnerability be demonstrated before applying the resolution.
3. If vulnerability information has been released and a grace period exists, then the customer should apply the resolution to its system during the grace period immediately.
4. Where possible, the customer should test any patches, configuration changes, or workarounds on test systems before making the changes in an operational environment.
5. The customer should inform the vendor and the public if a patch, configuration change, or workaround does not appear to work as described.
6. The customer should give preference to products whose vendors follow responsible disclosure practices.

VULNERABILITIES VERSUS EXPOSURES

For the purposes of this process, a security vulnerability is a flaw within a software system that can cause it to work contrary to its documented design and which could be exploited to cause the system to violate its documented security policy.

The following guidelines, while imprecise, provide the basis of a security vulnerability definition. A security vulnerability is a state in a computing system (or set of systems) which may:

- Allow an attacker to execute commands as another user
- Allow an attacker to access data that is contrary to the specified access restrictions for that data
- Allow an attacker to pose as another entity
- Allow an attacker to conduct a denial of service

The following guidelines provide the basis for a definition of an "exposure." An exposure is a state in a computing system (or set of systems), which is not a universal vulnerability, but may:

- Allow an attacker to conduct information gathering activities
- Allow an attacker to hide activities
- Include a capability that behaves as expected, but can be easily compromised
- Be a primary point of entry that an attacker may attempt to use to gain access to the system or data
- Be considered a problem according to some reasonable security policy

REFERENCES

- This policy also attempts to follow the [Guidelines for Security Vulnerability Reporting and Response](#) developed by the [Organization for Internet Safety](#).
- This policy is largely based on the Internet-Draft, [Responsible Vulnerability Disclosure Process](#), by Steve Christey and Chris Wysopal.
- Portions of this policy are also based on [Full Disclosure Policy \(RFPolicy\) v2.0](#) by Rain Forest Puppy
- This policy employs elements of the framework developed by the National Infrastructure Advisory Council (NIAC) as set forth in the [Vulnerability Disclosure Framework Report](#).

