Symantec Corporation™

Symantec Software Security Vulnerability Management Process

Best Practices
Roles & Responsibilities

INSIDE

INSIDE

Copyright © 2016 by Symantec Corporation

Disclaimer

Table of Contents

Overview

Security vulnerabilities in operating systems and applications continue to impact the online world. Exploits created to take advantage of these security vulnerabilities can lead to system compromise, non-availability, data loss, exposure of confidential information, and much more.

Educating development staff on secure coding practices can greatly reduce the chance of creating vulnerabilities, but it does not completely eliminate the problem. New methods of detecting and exploiting security issues are constantly being developed.

Symantec Corporation recognizes the importance of properly managing vulnerabilities discovered in its products to protect customers and the Internet community from potential security concerns.

This document describes Symantec's practice for responsible handling and disclosure of vulnerabilities discovered in Symantec products. It further outlines the communication and coordination process between Symantec and the individuals or organizations who report product vulnerabilities to us.

Vulnerabilities and Exposures

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

Vulnerabilities can allow attackers to:

- Execute commands as another user
- Access data that is contrary to the specified access restrictions for that data
- Pose as another entity
- Deny normally authorized access either completely or partially (Denial of Service)

Roles

Vendor

The vendor is the owner of the software. As a vendor, Symantec is responsible for verifying and correcting vulnerabilities found in our currently supported software. Symantec will also identify and implement a method for distributing corrective actions, fixes or updates, as appropriate. Symantec will also maintain an open working relationship with the finder who reported the vulnerability.

Finder

The finder is an individual or organization that identifies vulnerabilities in a vendor's product. When vulnerabilities are detected, the finder should document the vulnerability thoroughly, including information about the product version, test environment, and detailed steps to reproduce to ensure the vendor is able to replicate the reported findings. The finder should send this information, as well as any proof-of-concept they may have developed, to the vendor. The finder should maintain an open working relationship and lines of communication with the vendor through resolution of the issue and public release of any associated documentation.

Symantec Software Security Vulnerability Manager

The Symantec Software Security Vulnerability Manager is responsible for facilitating communication between the finder and Symantec's affected product groups during the resolution process. The Symantec Software Security Vulnerability Manager will provide timely status updates to the finder and will work with the finder to coordinated appropriate public notification.

Contact Information

Information on contacting the Symantec Software Security Vulnerability Management team is located at http://www.symantec.com/security/. This page includes a copy of the current Symantec Vulnerability Management PGP key and email address, secure@symantec.com, for submitting product vulnerability information concerning Symantec products.

Public Disclosure

Full Disclosure

All information, including details on how to exploit the vulnerability and proof-of-concept code, are published when discovered.

Because of the short period in which exploits can be created once full vulnerability information is published and the resultant risk to our customers, Symantec does not support full disclosure.

Responsible Disclosure

Symantec is a Responsible Disclosure company. Under responsible disclosure, the vendor is first notified privately by the finder of vulnerabilities they have discovered. All details including proof-of-concept code (if available) are shared with the vendor. The vendor is given a reasonable period of time to fix the vulnerability and release updates along with any mitigations. A reasonable time period for the resolution and disclosure window may range from 45 up to180 days under responsible disclosure guidelines depending on the range of products affected and the level of effort required addressing the findings submitted by the finder. The public notification in the form

of a security advisory is released publicly. The finder is credited for discovering the issue and reporting it to the vendor.

Symantec is a Responsible Disclosure company. As a founding member of the Organization for Internet Safety (OIS) we helped create the first formal Responsible Disclosure Guidelines. These guidelines encourage open communication between finders and vendors by clarifying the resolution process and responsibilities of each party. Symantec follows disclosure processes outlined in "ISO 29147, Information technology — Security techniques — Vulnerability disclosure" [ISO/IEC 29147:2014(E)], which greatly limits the risk to customers as updates are available for any public release of a vulnerability being addressed.

Symantec does not participate in a Bug Bounty Program. However, Symantec always provides full credit in our public advisories to all finders that work responsibly with us to resolve reported issues.

The Process

The process described below is a guide for handling security issues which encourages a good working relationship among all parties. The goal is to develop timely and effective resolutions to the identified vulnerability and offer the best risk protection to users of the affected software.

Initial Contact

Finders who believe they have discovered vulnerability in a Symantec product or products should contact the Symantec Software Security Vulnerability Management team through secure@symantec.com. To protect the user community, Symantec requests that the finder follow the responsible disclosure process and not post any information in public forums until after their submission is resolved and product updates are released and available to customers.

Preliminary Evaluation and Acknowledgment

The Symantec Software Security Vulnerability Manager will review the submission and send an initial timely acknowledgement to the finder and coordinate any additional information that may be required to complete the validation of the finder's issue. The Symantec Software Security Vulnerability Manager will inform the finder that the vulnerability information has been provided to the responsible team(s) within Symantec for review and verification.

Vulnerability Evaluation

After a vulnerability report has been reviewed, the Symantec Software Security Vulnerability Manager will forward the report to all affected product groups and our Software Security engineers for evaluation. Each product group will validate the issue and verify whether currently supported products are affected and, if so, which versions and develop a resolution plan. If additional information is required to reproduce the issue, the Vulnerability Manager will coordinate with the

finder to obtain additional information.

Vendor Coordination with Finder

The initial vulnerability and threat evaluation results will be communicated to the finder. If Symantec determines that our products are not affected by the vulnerability, the non-confidential information related to the review will be shared with the finder. If one or more Symantec products are affected by the security issue, the Symantec Software Security Vulnerability Manager will aid in coordinating a plan of action to resolve the issue and release public communication concerning the vulnerability. The Symantec Software Security Vulnerability Manager will maintain coordination with the finder throughout the resolution process.

Public Notification

Symantec will coordinate the release of a Symantec Product Security Advisory for the validated vulnerability with the finder. Symantec Security Advisories are posted on the Symantec Security Response web site. Many finders will publish their own advisory with a link to the vendor's advisory. Ideally, the advisories are coordinated during the release to avoid any confusion. Symantec works closely with researchers who identify vulnerabilities to us. When the security advisory is published, the finder is given full credit in our public advisory for reporting the issue to Symantec and working with us as we resolve the issue.

Threat Evaluation

A threat evaluation can help identify the severity of the vulnerability. The threat level should be based on the probability that the vulnerability will be exploited, method of exploit, and the potential resulting damage. The threat evaluation should include enough information to justify the specific level chosen and identify potential exploits that could be used to take advantage of the vulnerability.

Symantec currently uses the Common Vulnerability Scoring System (CVSS-SIG)[1] to identify the threat level of identified vulnerabilities. The CVSS calculates a score based on exploitability and impact metrics from known details of the identified vulnerability. The score is a number between 0 and 10 with 10 being the highest severity. From this score, Symantec Vulnerability Managers derive the following three severity classifications:

Low (0-3.9) – It is unlikely that this vulnerability will be exploited, cause serious damage or expose confidential information.

1. The Common Vulnerability Scoring System is a community standard for determining vulnerability threat levels. Symantec played a significant role in the creation of the CVSS.

Medium (4-6.9) – There is a reasonable chance that the vulnerability may be exploited, causing moderate damage, disrupt service, or expose confidential information.

High (7.0-10) – It is very likely that this vulnerability will be exploited, causing serious damage, disrupt service or compromise the targeted system and expose confidential information.

Conclusion

Symantec believes strongly in its responsibility to resolve vulnerabilities identified in our products. Symantec is committed to resolving security vulnerabilities quickly and thoroughly, culminating in the release of a Symantec Product Security Advisory and any required product update(s).

Symantec's position is that we are responsible for disclosing vulnerabilities discovered in our products but, in general, no vulnerability should be announced until we have developed and thoroughly tested a fix or mitigation and announced its availability to customers.

Because our products are complex, inter-related, and used on a variety of hardware under many different configurations, Symantec cannot always provide software security patches according to a set timeline. Each issue requires investigation, resolution, localization, and testing appropriate to its complexity. Development teams expedite security fixes as critical defects and will often work round-the-clock to deliver a sound patch should a serious vulnerability be found.

Responsible disclosure guidelines suggest that customers have an obligation to patch their systems as quickly as possible. Security updates, may be reverse engineered to identify how to exploit the vulnerability. Therefore, customers need to patch promptly.

Responsible security researchers work with the Symantec Software Security team through the email address secure@symantec.com. Responsible finders understand that the customer's security is paramount, so they work closely with Symantec to make sure fixes are available prior to publishing their own details regarding the vulnerability (ies) reported to Symantec.