Quick Heal Technologies Limited

Vulnerability Disclosure Policy

Definition

- "Company" or "Quick Heal" means Quick Heal Technologies Limited and includes its Seqrite Brand.
- "Third Party" means Vendors, Service Providers, Partners of Company.
- "Finder" means the security researcher, Customer, or other interested person or organization, who at the first instance identifies and reports the Vulnerability.
- "Quick Heal Products" means Security Software products manufactured by Quick Heal and includes the products manufactured under Seqrite brand.
- "Vulnerability Reward Program" shall means the program allied with this Vulnerability Disclosure Policy and defines the scope and terms and conditions for claiming rewards for disclosure of vulnerability(s) under this Policy.

Introduction

Company is one of the leading providers of security software products ("Quick Heal products") and solutions in India. Company believes that the process of vulnerability disclosure is a shared responsibility best practiced in strong coordination between the Company, finders, vendors, and protection providers working together to protect customers, businesses, and critical infrastructure.

Company's Approach to Vulnerability Disclosure Policy

Under the policy of Vulnerability Disclosure, finders shall disclose newly discovered vulnerabilities in software and services directly to the Company privately and exclusively in Company's preferred Email ID: secure@quickheal.com. The finder allows the Company with opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public or else. The Company continues to coordinate with the finder throughout the vulnerability investigation and provides the finder with updates on case progress. If attacks are underway in the wild, and the Company is still working on the update, then both the finder and vendor work together as closely as possible to provide early public vulnerability disclosure to protect customers. The aim is to provide timely and consistent guidance to customers to protect themselves.

Purpose of This Document

This document outlines Company's approach to Responsible Vulnerability Disclosure in two separate roles: finder and vendor. Company acts as finder where Company finds and reports some vulnerability in the third party's products/services. Company also acts as a vendor, when vulnerabilities that affect Company's products and services are reported by external finders.

This document aims to clarify how Quick Heal communicates the disclosure of vulnerabilities with industry peers, customers, and the research community in a responsible way. Lastly, this document explains how to engage with Quick Heal for coordinated vulnerability disclosure, when Quick Heal is acting in any of the two roles of finder and vendor. Quick Heal endeavors to follow this approach with every scenario whenever

possible.

1. Company as a Finder of Vulnerabilities

Process

Company may proceed with reporting of vulnerabilities that the Company finds in non-Quick Heal or third-party products and services that could impact the security of the Quick Heal (For the purpose of this section the term “third-party” refers to the party who owns the vulnerable product or service). The Vulnerability will be reported electronically or otherwise to the latest contact of the Third Party as available with the Company., which may include but not limited to the below mentioned elements:

- The known technical details of the vulnerability.
- The security impact to systems affected by the vulnerability.
- Severity of Vulnerability.
- Proof of Concept or Exploit Code.
- The technical root cause of the vulnerability (whenever available)

Any vulnerability information provided to the Third Party is not intended for public use, but for their use to identify and remediate the vulnerability. While some Third parties may have a standard, public e-mail address for the reporting of vulnerability, then the relevant contact will be used for communication.

In order to minimize the risk of vulnerability information being misdirected while attempting to identify the Third party’s contact, Company will not send the vulnerability report in the initial communication. The initial communication will be a simple introduction stating that we are attempting to identify the correct contact to report vulnerability in the Third Party’s products or services. When the appropriate contact is identified and confirms willingness to accept the vulnerability report, Company will provide the vulnerability report.

When the Third Party receives the vulnerability report, Company shall assume that they will begin investigating the issue. On being asked for assistance, Company may in turn, to the best of its ability, answer any technical questions that the third party may have. During this phase, Company periodically may ask the Third party, via e-mail or otherwise, for an update as to the progress of the resolving process and a best estimate of a timeline to develop remediation. In addition, upon request and if Company has resources available, Company may strive to provide some testing and comments on the effectiveness of the planned remediation of the vulnerability. This can be particularly important because an ineffective remediation could introduce new vulnerabilities or foster regressions.

Once the vulnerability is resolved the final step shall be alerting users of the affected product or service to the existence of the vulnerability and its risk. If the Third Party does not have an alerting process for users of the risk associated with the vulnerability and the available remediation, then Company will provide guidance on how users of the product or service can protect themselves.

Under no circumstances will Company release details of an unpatched vulnerability unless evidence of public attacks exists. In the event of public attacks, Company may also work with its partners to provide protection if a Third Party’s supplied remediation is not available.

Three main scenarios where Company may issue an advisory prior to the Third party's release of its own remediation are as follows:

- **When vulnerability technical details have become publicly known.**
- **When evidence of exploitation of an unpatched vulnerability surfaces.**
- **When the vendor fails to respond.**

2. Company as an Affected Vendor

In the case where Company is the vendor affected by vulnerability, then finders shall submit vulnerability reports to Company in the official Email ID i.e. secure@quickheal.com, which shall include but not limited to below mentioned information and elements:

1. Description and Type (Buffer Overflow, XSS, Access Control etc.) of the issue.
2. Severity and Impact of the issue.
3. Product and version.
4. Instructions and procedure to reproduce the issue including any additional information like:

    a) Operating System details including Service packs, security updates, or other updates for the product you have installed wherever relevant;
    b) Any special configurations required to reproduce the issue.

5. Proof-of-concept or exploit code.

A response would be sent within **5 business days** of receiving a creditable vulnerability report on the above email address to acknowledge that we have received the report.

Quick Heal takes immediate action on the vulnerabilities deemed critical and would release the fix on priority. However, depending on the Severity and Impact of the reported vulnerability Quick Heal **generally fixes** it within in **a period of 30-90 days**. In certain cases, due to the complexity involved to fix the vulnerability might go beyond the 90-day period. In such cases, Quick Heal would coordinate with the finder and keep them up-to-date on the plan.

Being that the ultimate goal is to fix the vulnerability in a manner that reduces risk to users the most, the goals of Company are as follows:

- Assess the overall risk of the vulnerability report.
- Collaborate with the finder to understand and reproduce the vulnerability.
- Maintain communication with the finder on the progress of the case through the investigation, remediation, and testing process.
- Ensure that the finder understands Company's position on Vulnerability Disclosure Policy.
- Facilitate communications, as required, between the finder and the necessary internal Company's team.
- Ensure that the finder, upon working in a coordinated manner with Company, receives proper credit for reporting and collaboration.

In case any vulnerability is found in any Websites, Web links and/or Blogs which are maintained and operated by Quick Heal, the same procedure of reporting and responding shall be followed as mentioned in this Policy.

As Quick Heal believes in honoring and appreciating all the cutting-edge external contributions and efforts that help us to keep our users safe, Finder(s) may be rewarded at the sole discretion of the Company, once the vulnerability is reasonably proven and validated.

Note:

1. The Finder shall maintain the confidentiality of relevant vulnerability report and shall not disclose this information anywhere without prior written consent by the Company.
2. Reward program under this Policy shall be governed by the then current "Vulnerability Reward Program" of the Company. The link to the said Vulnerability Reward Program is provided herein below:

   Vulnerability Reward Program

Conclusion

While no document can envision every vulnerability scenario, these practices are intended to provide greater clarity and certainty when coordinating vulnerabilities with Company. Company encourages other companies and security researchers to adopt a similar approach, and work with software providers to help minimize customer risk. By working together in a coordinated manner, we are creating a safer, more trusted computing experience for our customers.

Quick Heal solely reserves the right to amend and/or update this Policy at its own discretion without any prior intimation or notice, which shall be binding on all the Parties.

This policy is effective from **30th June 2016**.