Vulnerability Disclosure Policy

Tenable

December 2018

Version 1.5

Table of Contents

Vulnerability Disclosure Policy

Vulnerability Disclosure Purpose

The main goal of our vulnerability disclosure policy is to help ensure that vulnerabilities are patched or fixed by vendors in a timely manner with the ultimate objective of securing customers and the larger community while giving vendors adequate notice to provide a solution.

Due the large amount of effort poured into offensive security, Tenable firmly believes the maxim, "If we found it then someone else will too." This belief brings a sense of urgency to all findings and guides the timelines we outline below.

Vulnerability Disclosure Process

Initial Contact

Tenable will make attempts (within reason) to establish communication with the vendor's security team.

1. We will attempt to identify the official contact details for the vendor's security team to submit discovered vulnerabilities
2. If we are unable to identify an official means of contact for the security team, we will try to initiate contact via the standard customer support mechanism

Wherever required, our communication will transpire over encrypted email. The vendor will be provided with the necessary details of the discovered vulnerability, as well as a notification that the planned disclosure date is 90 days from when the initial contact attempt was made. Tenable will try to establish communication with the vendor three times:

1. The initial attempt
2. A second attempt after no less than one week after the initial attempt
3. A third attempt no less than two weeks after the initial attempt

If no response is received from the vendor within 45 days of the initial attempt, Tenable will notify CERT[1].

[1] Carnegie Mellon University Software Engineering Institute CERT https://www.sei.cmu.edu/about/divisions/cert/index.cfm

Working Together

Tenable is committed to working with vendors to help fix vulnerabilities. Tenable's policy is to be professional and helpful in our communications. Given our collective goal of helping to keep systems and data safe, the expectation is that vendors will return the same courtesy in their interactions with us. Tenable has a vested interest in being informed of the ongoing status of the Vendor's response to the submitted vulnerability and efforts in providing a solution.

Regular updates are not only appreciated but expected. This includes notifications and updates on:

- When the vulnerability has been confirmed
- When it has been passed to the development team
- When a patch(es) are planned to be released as well as when they are released
- Any other pertinent information relating to the efforts of the Vendor in addressing the reported vulnerability

Note: For purposes of this policy, the word patch encompasses software fixes for vulnerabilities as well as other forms of remediation or mitigation provided by the vendor.

This policy will continue to be in effect even if the vendor has prior knowledge of the vulnerability disclosed by Tenable.

Tenable also recognizes that external messaging may be important to the vendor. If desired, our public relations team will work with the vendor to develop joint press releases or synchronize on messaging (within the timelines established in this policy).

Going Public

Barring extenuating circumstances, Tenable will publish a security advisory with full technical details and a proof of concept (if available) on the first business day after the 90 day period has lapsed regardless of whether the vendor has released a patch.

If a 90-day disclosure date is approaching but a vendor lets us know in advance that a patch is forthcoming on a specific day within 14 days following the planned disclosure date, the security advisory will be delayed until the availability of the patch or the expiry of the 14 day grace period, whichever is earlier.

If the vendor releases a patch or security advisory prior to the 90 day timeframe, Tenable may also release an advisory with full technical details and a proof of concept (if available) prior to the planned disclosure date.