Vulnerability Disclosure Policy

Tenable

March 2022

Version 1.9

Tenable, Inc.

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 to 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 email communication with the vendor's security team. If we are unable to identify an official email for the security team, we will try to initiate contact via the standard customer support mechanism.

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 an adequate response is not received from the vendor within 45 days of the initial attempt, Tenable will publicly disclose the issue(s) and / or address as it is deemed fit.

If an appropriate security contact can be established, the contact will be provided with information about the discovered vulnerabilities, a link to this policy, a tracking identifier, and a notification that the planned disclosure date is 90 days from when the vulnerabilities were disclosed to the vendor or other reporting authority.

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 can work with the vendor to develop joint press releases or synchronize on messaging (within the timelines established in this policy).

Going Public

Tenable publishes Security Advisories (each, a "Security Advisory") with known technical details and a proof of concept (if available). Barring extenuating circumstances, Tenable shall adhere to the following cadence with regards to publication of Security Advisories.

Tenable may publish Security Advisories on the first business day following either: (i) a 90-day period commencing on Tenable's disclosure of the vulnerability to the vendor; or (ii) a 45-day period commencing on the date of Tenable's first attempted contact of the vendor if reasonable contact was unable to be established. Tenable may publish such Security Advisory regardless of whether or not the vendor has released a patch.

If the vendor does release a patch, security advisory, or any other information regarding the vulnerability either publicly or to any of its partners or customers prior to the 45 or 90 day timeframe, Tenable may release a Security Advisory prior to its planned disclosure date.

If a vendor releases a patch either publicly or to any of its partners or customers that is later found to be incomplete (by Tenable or otherwise), Tenable will promptly make a good faith attempt to notify the vendor. Tenable may publicly disclose the incompleteness of such a patch 7 days after the attempt is made. If the details of an incomplete patch become public during this interim 7-day period, Tenable may release known details immediately.

If Tenable discovers a vulnerability which is: (i) being actively exploited in the wild at any stage of the disclosure process; and (ii) is not yet public information (i.e. via a blog, advisory, news article, media mention, etc.), then Tenable may release a full Security Advisory with known technical details 7 days after attempting to notify the vendor about the exploitation. If the vulnerability details become public in that interim 7-day period, Tenable may release a Security Advisory with known technical details immediately.

Tenable's Zero Day Research team can be reached at bughunters@tenable.com.