Vulnerability Disclosure Policy

Tenable

November 2023

Version 2.0

Tenable, Inc.

Copyright 2023 Tenable, Inc. All rights reserved. Tenable is a registered trademark of Tenable, Inc.

Table of Contents

Vulnerability Disclosure Purpose 3

Vulnerability Disclosure Process 3

Initial Contact 3

Working Together 4

Going Public 4

Copyright 2023 Tenable, Inc. All rights reserved. Tenable is a registered trademark of Tenable, Inc.

Vulnerability Disclosure Policy

Purpose

The primary objective of this Vulnerability Disclosure Policy (this "Policy") is to help ensure that vulnerabilities are patched or fixed by vendors in a timely manner in order to increase operational security for customers and the larger community. Ultimately, this Policy strives to balance this goal with the need to provide vendors with adequate notice to provide effective solutions.

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 acts to guide the timelines outlined below.

Process

Initial Contact

Tenable shall make commercially reasonable attempts 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 shall try to establish communication with the vendor three times:

1. The initial attempt;
2. A second attempt after no less than one week of the initial attempt; and
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 may publicly disclose the issue(s) and/or address as Tenable in its sole judgment deems appropriate.

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.

Copyright 2023 Tenable, Inc. All rights reserved. Tenable is a registered trademark of Tenable, Inc.

Working Together

Tenable is committed to working with vendors to help fix vulnerabilities and therefore we strive 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 associated 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 the vulnerability has been passed to the development team;
- When a patch(es) is planned to be released as well as when they are actually released; and
- 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, the Tenable public relations team can cooperate in good faith with the vendor to develop joint press releases or collaborate 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) the 90-day period commencing on Tenable's disclosure of the vulnerability to the vendor; or (ii) the 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.

Copyright 2023 Tenable, Inc. All rights reserved. Tenable is a registered trademark of Tenable, Inc.

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.

Tenable recognizes the sensitive nature of vulnerability disclosure surrounding critical infrastructure and operational technologies. Therefore, when deemed appropriate by Tenable, and at times in cooperation with the vendor, Tenable may withhold certain technical details such as proof of concept exploit code in order to protect our customers and the general public.

Tenable, Inc. reserves the right to deviate from this Policy in its discretion.

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

Copyright 2023 Tenable, Inc. All rights reserved. Tenable is a registered trademark of Tenable, Inc.