Vulnerability Disclosure Policy

This document describes the security vulnerability disclosure policy of VoidSec.

This is the official policy of VoidSec (referred to as “us” or “we” hereafter) to exercise the responsible/coordinated disclosure of security vulnerabilities in a manner which is of maximum value to all affected parties. VoidSec reserves the right to change this policy at any time and at its sole discretion, without prior notice. The updated version of the policy can be retrieved at any time at: https://voidsec.com/disclosure-policy/

Current version: v2.0, last changed on February 19, 2021, 11.18

This policy sets out the ‘guidelines’ that we intend to follow.

Policy definitions

The **ISSUE** is the vulnerability, bug, problem, or otherwise reason for contact and communication between the **REPORTER** and the **VENDOR(s)**.
The **REPORTER** is the individual or group submitting the **ISSUE**.
The **VENDOR** is the individual, group, or company that maintains the software, hardware, or resources that are related to the **ISSUE**.
The **DATE OF CONTACT** is the point in time when the **REPORTER** contacts the **VENDOR**.
The **DATE OF PUBLIC DISCLOSURE** or **DISCLOSURE DATE** is the point in time when we disclose the vulnerability to the general public.
All dates, times, and time zones are relative to the **REPORTER**.

In case where a VENDOR is unresponsive or does not establish a reasonable timeframe for ISSUE remediation, we may disclose vulnerabilities 30 days after the DATE OF CONTACT, regardless of the existence or availability of patches or workarounds from the affected VENDOR.

We will always attempt to coordinate all reported vulnerabilities with the affected VENDOR.

We strongly believe that coordinated disclosure is the best approach to properly and efficiently address a vulnerability and thus protect VENDORs’ customers. However, software VENDORs too often deliberately fail to respond to vulnerability reports submitted by security researchers (not respecting the valuable work performed by them), or simply take too long to develop fixes, thus irresponsibly leaving their customers exposed to vulnerabilities for a long period of time.

Based on years of experience with VENDORs of various sizes having different approaches and attitudes towards vulnerabilities fixing, we have decided upon this disclosure policy which we deem a reasonable “compromise” between a fair amount of engineering and quality assurance efforts and the need of providing a timely fix to vulnerabilities.

Vulnerabilities reported to us by REPORTERs will be disclosed to the general public 30 days after the DATE OF CONTACT, regardless of the existence or availability of patches or workarounds from affected VENDORs. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. Disclosures will include credit to the REPORTER unless otherwise requested. We will communicate to any affected VENDORs of our publication plans, and negotiate alternate publication schedules with the affected VENDORs when required.

Since this policy aims to balance the interest of the general public to be informed of security vulnerabilities with the VENDORs' need for time to respond effectively, the final determination of a publication schedule will be based on the best interests of the community overall.

Vulnerabilities reported to us will be forwarded to the affected VENDORs as soon as we receive and process the report. The name and contact information of the REPORTER will be forwarded to the affected VENDORs unless otherwise requested. We will advise the REPORTER of significant changes in the status of any vulnerability reported without disclosing confidential information provided to us.

For projects that have a public bug report page, we cannot guarantee any disclosure time (or responsible disclosure), as anyone having access to the bug report has also the access to the vulnerability. In this case, we will evaluate a possible immediate publication (full disclosure) to promote a more rapid fix.

Workflow

1. If no security contact is known for the VENDOR, an e-mail requesting the security contact e-mail address may initially be sent to certain public e-mail addresses associated with the VENDOR. It is our policy to never submit vulnerability information via online forms. However, these may be used to request security contact information. This document is always attached, as PDF file or link, during the first contact made with the VENDOR.
2. If the VENDOR does not reply with a security contact or other relevant e-mail address within a week, it is our policy to set the DATE OF CONTACT to that day. The DISCLOSURE DATE is set 30 days after the DATE OF CONTACT.
3. When a security contact or other relevant e-mail address has been identified, a VENDOR initially receives an e-mail with vulnerability details along with a preset DISCLOSURE DATE (usually 30 days later the DATE OF CONTACT).
4. If the VENDOR does not respond to the initial e-mail within a week, the e-mail is resent.
5. If no response has been received on the day of the DISCLOSURE DATE, the vulnerability is published immediately without further coordination attempts.
6. If the VENDOR responds to either the initial e-mail or the resent e-mail, a new DISCLOSURE DATE may be set in case the VENDOR cannot meet the preset date.
7. We expect VENDORs to provide continuous status updates. If none are provided by default, the VENDOR will be contacted about once a week with a status update request.

8. Should the VENDOR not respond to two consecutive status update requests, an e-mail is sent to the VENDOR advising that the vulnerability information will be disclosed a week later. If no further response has been received by that date, the vulnerability information will be immediately published without further coordination attempts.
9. Eventually, the vulnerability information will be published by us when:
    1. The preset/agreed DISCLOSURE DATE is reached.
    2. The VENDOR issues a fix and/or security advisory.
    3. Information about the same vulnerability is published by a third party.
10. By default, vulnerabilities are coordinated for no more than 30 days.
11. A vulnerability DISCLOSURE DATE may in certain cases be coordinated if the VENDOR is communicating a clear intention to address the vulnerability and can commit to a fixed date and the vulnerability is considered to be complex to address.
12. In respect of the REPORTER, the VENDOR is encouraged to provide proper credit to the REPORTER submitting the ISSUE.
    Suggested (minimal) credit would be:
    "Credit to [REPORTER], a member of VoidSec, for submitting the vulnerability to [VENDOR] and working with us to protect our customers."
13. The VENDOR is strongly encouraged to coordinate a joint public release/disclosure with VoidSec, so that security advisories can be made jointly available.