Vulnerability Disclosure Policy

v.1.1

This document describes the security vulnerability disclosure policy of VoidSec Team Members.

It is the official policy of VoidSec Team Members (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, without prior notice.

Current version: v1.1, last changed on August 12, 2013, 16:30

The permalink URL for this policy is http://voidsec.com/disclosure-policy/

This policy states the 'guidelines' that we intends to follow.

Policy definitions

The **ISSUE** is the vulnerability, problem, or otherwise reason for contact and communication.
The **REPORTER** is the individual or group submitting the **ISSUE**.
The **VENDOR** is the individual, group, or **VENDOR** 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**.
All dates, times, and time zones are relative to the **REPORTER**
The **DATE OF PUBLIC DISCLOSURE** is the point in time when the **VoidSec Team** disclose the vulnerability to the public.
All dates, times, and time zones are relative to the **REPORTER**.

NB: In cases where a VENDOR is unresponsive, or will not establish a reasonable timeframe for remediation, VoidSec Team Members may disclose vulnerabilities 30 days after the DATE OF CONTACT is set, regardless of the existence or availability of patches or workarounds from affected VENDORs.

VoidSec Team Members will attempt to coordinate all reported vulnerabilities with the affected VENDOR.

We strongly believes that a coordinated disclosure is the best approach to properly and efficiently address a vulnerability and thus protect a VENDOR's customers. However, software VENDORs too often deliberately fail to respond to vulnerability reports, don't respect the valuable work made by the researcher, or simply take too long to develop fixes thus leaving their customers exposed for an irresponsibly long period of time.

Based on years of experience with VENDORs of various sizes having various approaches and attitudes towards fixing vulnerabilities, we have decided upon the following disclosure policy, which we find to be a reasonable "match" between a fair amount of engineering and quality assurance efforts and the need of providing a timely fix to vulnerabilities.

Vulnerabilities reported to us will be disclosed to the 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 made by us will include credit to the REPORTER unless otherwise

requested by the REPORTER. We will apprise any affected VENDORs of our publication plans, and negotiate alternate publication schedules with the affected VENDORs when required.

It is the goal of this policy to balance the need of the public to be informed of security vulnerabilities with 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 practical after we receive the report. The name and contact information of the REPORTER will be forwarded to the affected VENDORs unless otherwise requested by the REPORTER. We will advise the REPORTER of significant changes in the status of any vulnerability he or she reported to the extent possible without revealing information provided to us in confidence.

For projects that have a public bug report page we cannot guarantee any disclosure time (or responsible disclosure), as anyone who has access to the bug report has the access to the vulnerability. In this case we 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.
2. If the VENDOR doesn't reply with a security contact or other relevant e-mail address within a week is our policy to set the DATE OF CONTACT to that day. The disclosure date is set to the first Saturday 30 days later after the DATE OF CONTACT.
3. When a security contact or other relevant e-mail address has been identified, a VENDOR initially receives a mail with vulnerability details along with a preset disclosure date (usually set to the first Saturday 30 days later).
4. If the VENDOR does not respond to the initial mail within a week, it is resent.
5. If no response has been received at the day of the preset disclosure date, the vulnerability information is published immediately without further coordination attempts.
6. If the VENDOR responds to either the initial mail or the resent mail, a new disclosure date may be set in case the VENDOR cannot meet the preset date.
7. We expects VENDORs to provide continuous status updates on the progress. If none are provided by default, the VENDOR will be contacted about once a month with a status update request.
8. Should a VENDOR not respond to a status update request, it is resent a week later.
9. Should the VENDOR not respond to two consecutive status update requests, a mail is sent to the VENDOR advising that the vulnerability information will be disclosed a week later if no response is received. If no further response has been received by this date, the vulnerability information is immediately published without further coordination attempts.
10. Eventually, the vulnerability information will be published by us when:
    a. The preset/agreed disclosure date is reached.
    b. The VENDOR issues a fix and/or security advisory.
    c. Information about the same vulnerability is published by a third party.
11. By default, vulnerabilities are coordinated for no more than 30 days.
12. A vulnerability may in certain cases be coordinated for up to one full year if the VENDOR is communicating a clear intention to address the vulnerability and can commit to a date within that period and the vulnerability is considered to be complex to address.
13. In respect for the REPORTER following this policy, the VENDOR is encouraged to provide proper credit to the REPORTER for doing so. Failure to document credit to the REPORTER may leave the REPORTER unwilling to follow this policy with the same VENDOR on future issues, at the REPORTER's discretion. Suggested (minimal) credit would be:
    "Credit to [REPORTER], a member of VoidSec Team, for disclosing the problem to [VENDOR] and working with us to protect our customers."
14. The VENDOR is encouraged to coordinate a joint public release/disclosure with the REPORTER and us, so that advisories of problem and resolution can be made available together.
15. All email communication from VENDOR to REPORTER and from REPORTER to VENDOR must be sent also to **security@voidsec.com.**

Frequently asked questions regarding this policy

Q: **Does this mean VoidSec Team Members are going "full disclosure?"**

A: We will not distribute exploits, if that's what "full disclosure" means. In our experience, the number of people who can benefit from the availability of exploits is small compared to the number of people who get harmed by people who use exploits maliciously. We will, however, disclose information about vulnerabilities that we might not have previously disclosed. Within the limits of our resources, we will publish information about as many vulnerabilities as we can.

Q: **Why not 45 days, or 15 days, or immediately?**

A: We think that 30 days can be a pretty tough deadline for a large organization to meet. Making it shorter won't realistically help the problem. In the absence of evidence of exploitation, gratuitously announcing vulnerabilities may not be in the best interest of public safety.

Q: **Wouldn't it be better to keep vulnerabilities quiet if there isn't a fix available?**

A: Vulnerabilities are routinely discovered and disclosed, frequently before vendors have had a fair opportunity to provide a fix, and disclosure often includes working exploits. In our experience, if there is not responsible, qualified disclosure of vulnerability information then researchers, programmers, system administrators, and other IT professionals who discover vulnerabilities often feel they have no choice but to make the information public in an attempt to coerce vendors into addressing the problem.

Q: **Will all vulnerabilities be disclosed within 30 days?**

A: No. There may often be circumstances that will cause us to adjust our publication schedule. Threats that are especially serious or for which we have evidence of exploitation will likely cause us to shorten our release schedule. Threats that require "hard" changes (changes to standards, changes to core operating system components) will cause us to extend our publication schedule.

Q: **Will you surprise vendors with announcements of vulnerabilities?**

A: No. Prior to public disclosure, we'll make a good faith effort to inform vendors of our intentions.

Q: **If a vendor disagrees with your assessment of a problem, will that information be available?**

A: Yes. We solicit and post authenticated vendor statements and reference relevant vendor information in vulnerability notes. We will not withhold vendor-supplied information simply because it disagrees with our assessment of the problem.

Q: **Who gets the information prior to public disclosure?**

A: Generally, we provide the information to anyone who can contribute to the solution and with whom we have a trusted relationship, including vendors (often including vendors whose products are not vulnerable), community experts, sponsors, and sites that are part of a national critical infrastructure, if we believe those sites to be at risk.

Q: **Do you disclose every reported vulnerability?**

A: We may, at our discretion, decline to coordinate or publish a vulnerability report.

Contact

If you have any questions about this policy, please contact **security@voidsec.com.**