Using Responsible Vulnerability Disclosure Programs to Manage Risk

Managing Disclosure of Vulnerabilities and Risk

The effect of a publicly disclosed cybersecurity breach or weakness can be substantial for any organization that cares about its reputation. It's not hard to find examples of public organizations who are in the news because of a vulnerability that leaked information or put constituents or partners at risk. However, there are ways to minimize the likelihood of such an occurrence for your organization.

What Is a Responsible Vulnerability Disclosure Program?

One such way is to create what's known as a Responsible Vulnerability Disclosure Program (or RVDP), also known as a Coordinated Vulnerability Disclosure or Responsible Disclosure Program. An RVDP provides guidance to security researchers, or people who discover a problem with your organization's use of technology, so that they can follow your approved process to notify you and get the issue fixed. RVDPs have become a standard way to avoid miscommunication, reputation impact, and other problems that have arisen when security researchers identify a flaw or weakness in an organization's cybersecurity posture. There are several online resources available to develop RVDPs, including disclose.io, which allows users to build a policy using the policy configuration tool found on the website.

Image recreated from graphic used on dislose.io

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

Providing Clear Instructions for Security Researchers

Security Researchers are usually self-motivated to understand technology and identify weaknesses that could put people at risk. This altruistic drive has been misunderstood in the past, and people have been prosecuted for attempting to disclose a situation that needed to be fixed. Recently, the US Justice Department announced that security researchers will no longer face prosecution for disclosure of vulnerabilities where such activity is carried out in a manner designed to avoid any harm to individuals or the public. While this change in policy creates a clear signal that ethical security research is no longer considered criminal in nature, it still leaves a wide range of questions unanswered about how researchers and organizations that are the subject of research might best resolve any issues discovered in a way that protects both parties.

This is where an RVDP becomes critical in managing risks surrounding disclosure by preventing impact to organizations due to untimely public disclosure of vulnerabilities. By providing clear and concise information that researchers can use to report a discovered vulnerability, and a process by which researchers can expect that the vulnerability will be addressed, organizations can mitigate a substantial amount of the risk associated with disclosure. Having a clearly-defined RVDP also discourages researchers from releasing sensitive information in a full-disclosure to the public before your organization has an opportunity to address any vulnerabilities that may harm your organization or its clients.

Creating a program can be as simple as using an online resource like disclose.io, using guidance from Federal authorities like the Cybersecurity & Infrastructure Security Agency (CISA). For organizations that require authorization for policies from higher authorities, your legal department should be consulted. Organizations may wish to simply direct any security researchers to CISA's Responsible Disclosure program, found at:

https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

Creating a Program Starts With Policy

When considering how to build a RVDP, organizations should begin by drafting policy that aligns with their bylaws and organizational charters. Critical elements of an effective policy include the following[3]:

- A Safe Harbor provision that provides clear description of acceptable disclosure practices and provides indemnification of activity that follows these practices;
- The method of communication or communication channel (e.g., email, web form, etc.) that should be used to communicate security findings;
- A hosting location where the policy will be published (e.g., website URL);
- A timeline that researchers can expect your organization to follow regarding when disclosures will be accepted, reviewed, acted upon, and how often communication between researchers and the organization might occur.

Publication and Public Notification

Publish the RVDP in a prominent digital location, such as a specific URL (e.g., https://yoursite.org/rvdp.html) and provide links to the published policy in your website's URL. Another great way to raise awareness of your RVDP is to publish posts on social media. It's also advised to produce a press release that covers your organization's adoption of responsible disclosure practices and point the reader to the location of your policy.

Some organizations may wish to have a third party such as CISA coordinate responsible disclosure efforts on their behalf. There are several organizations that serve as clearinghouses for vulnerability notifications, however the two most prominent are CISA.gov and the MITRE Common Vulnerability and Exploit website (cve.org). Organizations who choose not to produce a specific RVDP should consider posting a notice on their website that anyone seeking to responsibly report a vulnerability should contact CISA or use the CVE.org website. This allows researchers to attempt to follow responsible disclosure practices that are generally accepted by the community, using well known methods outlined on the respective vulnerability disclosure sites.

[1] Example prosecution of disclosed vulnerabilities, retrieved from https://www.washingtonpost.com/politics/2021/10/25/fight-missouri-shows-damage-overbroad-hacking-laws/, June 2022
[2] US Department of Justice policy change for CFAA, retrieved from https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act, June 2022
[3] Example policy created by disclose.io, retrieved from https://policymaker.disclose.io/policymaker/download/vdp, June 2022

Sample RVDP From Acme Inc Vulnerability Disclosure Policy

Introduction

Acme Inc welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

Systems in Scope

This policy applies to any digital assets owned, operated, or maintained by Acme Inc.

Out of Scope

Assets or other equipment not owned by parties participating in this policy.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor for your vulnerability research that is related to this policy.

Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;
- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Official Channels

Please report security issues via mailto:sample@acme.org, providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

Safe Harbor

When conducting vulnerability research, according to this policy, we consider this research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy;
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms of Service (TOS) and/or Acceptable Usage Policy (AUP) that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

Conclusion

Responsible Disclosure Vulnerability Programs are a significant risk reduction tool for organizations that use technology and are concerned about their online reputation and the protection of information systems and data. RDVPs allow both researchers and organizations under scrutiny to establish a communication protocol that provides a clear method of disclosure and resolution of security vulnerabilities. Given the recent ruling about security research, it is reasonable to expect more research will occur in the future, and having an RVDP in place will provide guidance for communicating a vulnerability discovered by a security researcher.

About Ingalls Information Security

Ingalls Information Security understands cybersecurity attacks and how to respond effectively. Since 2010, we've been in war rooms and boardrooms, investigating computer networks targeted and attacked by criminals and nation-state sponsored hackers. This experience gives us a powerful edge in preventing and responding to cyberattacks.

Ingalls helps businesses large and small manage security risks and defend against cyberattacks. If you'd like to learn more, please email us at contact@iinfosec.com or visit iinfosec.com. One of our cybersecurity experts will be more than happy to assist you and answer any questions you may have.

INGALLS
INFORMATION SECURITY
Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452