Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Vulnerability Disclosure Programs Explained

First published: November 2022
Last updated: December 2024

Introduction

A vulnerability disclosure program (VDP) is a collection of processes and procedures designed to identify, verify, resolve and report on vulnerabilities disclosed by people who may be internal or external to organisations. The importance of developing, implementing and maintaining a well thought-out VDP cannot be underestimated. It is an integral part of professional organisations' business operations. Implementing a VDP, based on responsible and coordinated disclosure, assists organisations, vendors and service providers by improving the security of their applications, products or services. In addition, following the confirmation and resolution of a reported vulnerability, a VDP may assist organisations in notifying their customer base of any potential risks associated with the use of their applications, products or services. Mitigation strategies in the form of patches and updates are underpinned by the development, implementation and maintenance of a robust VDP.

Importance and justification

New vulnerabilities are discovered regularly. As such, it is important for organisations to have a mechanism in place that makes the reporting of vulnerabilities quick and easy. VDPs provide the framework and guidance that enables this. Once a vulnerability has been disclosed, it can provide organisations with the information required to shape appropriate mitigation steps and decrease the chance of exploitation of the vulnerability by malicious actors. This information can also help organisations' management understand and address the risk that a vulnerability may pose to staff, end users and business customers. Outlined within this publication is the information necessary for organisations of all sizes to develop, implement and maintain a VDP that will improve their cyber security posture and decrease their organisational risk.

Bug bounty programs

VDPs are sometimes referred to as 'bug bounty programs'. A bug bounty program is a program that is usually designed by web developers or software engineers on behalf of organisations to encourage people to locate, identify and report on 'bugs' that may exist within organisations' information and communications technology (ICT) infrastructure in order to receive a 'bounty', such as a cash reward or public recognition. While any issue identified through a bug bounty program must be taken seriously, the discovery of a vulnerability should always be given priority and addressed as a matter of urgency. In the United States, the Pentagon uses a bug bounty program to encourage security researchers and security professionals to identify issues with its ICT infrastructure. This is all part of the Pentagon's overarching vulnerability disclosure strategy. Bug bounty programs, like the one developed by the Pentagon, remove the negative stigma often associated with unsolicited security testing while providing guidance for security researchers and security professionals on what forms of unsolicited security testing are and are not acceptable to organisations.

Vulnerability disclosure program development

Preparatory considerations

Before organisations can implement a VDP, they must first decide on the parameters of their program. At a minimum, this should include:

- the purpose of the program
- the types of security testing that may or may not be permitted
- how reporting will be undertaken in the event that any vulnerabilities are discovered
- associated timeframes and supporting actions for the notification of vulnerabilities
- expectations regarding the disclosure of vulnerabilities
- any recognition, reward or incentive for finders of vulnerabilities.

Essential elements

It is essential that the right information is developed and communicated within a VDP. At a minimum, a VDP should cover the following essential elements:

- an internal vulnerability disclosure policy
- an external vulnerability disclosure policy
- reporting and communication channels, including key points of contact.

Internal vulnerability disclosures

It is a good cyber security practice for organisations to regularly and systematically test their ICT infrastructure such that vulnerabilities, should they exist, are identified and mitigated quickly. Vulnerabilities that are identified and disclosed to organisations are usually discovered by security researchers or security professionals, such as someone who, with prior approval from organisations' management and legal advisors, is paid to intentionally search for and expose vulnerabilities within different parts of organisations' systems. This is usually done in the form of penetration tests, vulnerability assessments or vulnerability scans.

Implementation

Once an internal vulnerability disclosure policy has been successfully developed, it needs to be implemented and maintained. The steps below provide a guide that organisations can use to incorporate their internal vulnerability disclosure policy into standard business operations:

- Determine who will conduct penetration tests, vulnerability assessments or vulnerability scans. Will internal staff be used or will a third-party contractor or organisation be hired to complete the task?
- Identify which parts of the ICT infrastructure will be tested. For example, management may only want to test one application, product or service as opposed to the whole ICT infrastructure.

- Determine how often penetration tests, vulnerability assessments or vulnerability scans will be conducted in support of the internal vulnerability disclosure policy. This should be determined by organisations' management and ICT departments.

- Establish a non-disclosure agreement with security researchers or security professionals who will conduct penetration tests, vulnerability assessments or vulnerability scans. This is an important aspect of VDPs and ensures information is only disclosed on agreed terms.

- Ensure that staff, end users and business customers are aware of the dates and times that penetration tests, vulnerability assessments or vulnerability scans are being carried out. This may need to be arranged in conjunction with ICT infrastructure maintenance periods.

- Develop a communication plan that outlines how vulnerabilities will be reported to staff, end users and business customers in the event that they are discovered. In some circumstances, organisations may also need a media engagement strategy. Having a communication plan in place will assist organisations to respond to an identified vulnerability by ensuring that the correct stakeholders are given the information they need in a timely manner.

- Consider providing appropriate rewards or recognition to people who identify vulnerabilities. This supports the development of a thriving security testing community while also contributing to fostering respect between organisations and the security testing community.

External vulnerability disclosures

Organisations that are informed of a vulnerability need to act quickly and decisively. Organisations need to be postured for success should a vulnerability be disclosed by an external source.

Implementation

The guidance below will support the development, implementation and maintenance of an external vulnerability disclosure policy:

- Every report should be taken seriously. As such, when a report is received the person who identified the vulnerability should be thanked. Positive reinforcement builds rapport which means the person may be inclined to help again in the future.

- Ensure the report is passed to the right people. This should include those that are responsible for the affected application, product or service. If this is a third-party provider, discuss the report with them directly.

- Where possible, pressuring the person who identified the vulnerability to sign formal documents, such as a non-disclosure agreement, should be avoided. Reassure them that the issue is being worked on and that it will be fixed as soon as possible.

- If more information is required to develop a comprehensive understanding of the vulnerability, politely request it from the person that identified it. Additional information will also assist technical specialists who may be required to fix the vulnerability.

- Once the appropriate people have been engaged, and decided on a course of action, the person that identified the vulnerability should be advised that the issue is being managed. In doing so, there is no need to disclose a lot of technical detail, or commit to a timeline, but maintaining contact is important.

- In the event that the vulnerability takes time to fix, periodic updates should be provided to the person that identified the vulnerability. Maintaining a good relationship with security researchers and security professionals is essential.

- Once the vulnerability has been rectified, the person that identified the vulnerability should be notified. At this point, it is highly likely that the person will be willing and able to re-examine the issue to confirm that the vulnerability has been resolved.

- Finally, publicly acknowledging and thanking the person who identified the vulnerability, if they want to be publicly identified, can create a sense of trust and transparency within the security researcher and security professional communities.

Reporting

Communication

After a vulnerability has been identified and verified, organisations have a responsibility, and sometimes a legal obligation, to release a vulnerability report. Reporting a vulnerability ensures that all relevant stakeholders can take necessary steps in response, such as performing updates or taking applications, products or services offline until an appropriate resolution can be applied. At a minimum, vulnerability reports should include what the vulnerability was, an assessment of its impact and what remediation steps need to be taken.

As part of reporting vulnerabilities, organisations should ensure that all communication is clear and concise, without any ambiguity. In doing so, vulnerability reports need to be written in a way that people with a non-technical background can understand what the issue is and how they might be affected. Example contents of a vulnerability report may include:

- an explanation of the vulnerability, including its impact
- applications, products or services affected
- potential end users affected
- potential mitigation steps to take
- ongoing remediation and security arrangements.

Security.txt

While it is best practice for organisations to have a dedicated point of contact for people, both internal and external, to raise vulnerabilities with, establishing and using a 'security.txt' file is strongly encouraged. A security.txt file is a communication mechanism that provides information on how organisations would prefer to receive reports of vulnerabilities from security researchers and security professionals. Organisations typically place a security.txt file in a standardised location on their website, such as yourorganisation.com/.well-known/security.txt.

The key components of a security.txt file, using example contents, are listed below:

- **Contact:** https://www.yourorganisation.com/contact (required - best contact email address for reporting vulnerabilities)
- **Expires:** 2023-12-31T01:59:00.000Z (required - date and time when the contents of the security.txt file will expire)
- **Encryption:** https://www.yourorganisation.com/pgp-key.txt (link to the public encryption key to use for secure communications)

- **Acknowledgements:** https://www.yourorganisation.com/acknowledgements (link to the list of people that have reported verified vulnerabilities)
- **Preferred-Languages:** English (a list of languages that the security team speaks)
- **Canonical:** https://www.yourorganisation.com/.well-known/security.txt (link to the security.txt file to enable digital signing)
- **Policy:** https://www.yourorganisation.com/security-policy (link to the external vulnerability disclosure policy)
- **Hiring:** https://www.yourorganisation.com/careers (link to security-related job vacancies in your organisation).

Cyber security culture

Cultivating awareness

Operating a VDP can help to build a strong cyber security culture within organisations. Specifically, if vulnerabilities are not proactively identified and mitigated, it is likely that organisations will experience a security issue at some point relating to their applications, products or services that potentially results in reputational damage or another form of business impact. As such, promoting a strong cyber security culture within organisations should be at the forefront of all modern business practices. By promoting a strong cyber security culture, employees, especially developers and engineers, will be more likely to remain vigilant in identifying and reporting vulnerabilities as set out within internal vulnerability disclosure policies.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Organisations can report vulnerabilities to the Australian Signals Directorate (ASD). Once a vulnerability is reported to ASD, it is recorded and triaged. At this time the priority and extent of assistance that is necessary to respond to the vulnerability is determined.

ASD takes the protection of information seriously. Under the limited use obligation, information voluntarily provided to ASD about cyber security incidents, potential cyber security incidents or vulnerabilities impacting organisations cannot be used for regulatory purposes.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate