Responsible Vulnerability Disclosure Policy

Responsible Vulnerability Disclosure ("**RVD**") is a process where a person/organisation responsible for a product or service (the "**System Owner**") is informed of a cybersecurity vulnerability in the product or system, in order that they may mitigate or eradicate the risk that the vulnerability may be exploited, and minimise or prevent potential harms that may result.

SingCERT supports RVD as a means of fostering cooperation between System Owner(s) and the wider cybersecurity community, so as to improve cybersecurity and build a trusted and resilient cyberspace.

SingCERT will act as a coordinator, whereby upon receiving a report from anyone that has identified or knows of a suspected vulnerability in a product or service (the "Informer"), we will assist in contacting and passing along the report to the System Owner(s). Where necessary and appropriate, we may put the Informer and System Owner(s) directly in touch, to enable better communication and coordination. SingCERT will not participate and/or be involved in the vulnerability verification process between the Informer and the System Owner(s). Informers understand and acknowledge that they submit vulnerability reports out of their own volition and there is no recommendation, endorsement, and/or compulsion on the part of SingCERT for Informants to participate in RVD and/or submit vulnerability reports.System Owner(s) are encouraged to develop their own vulnerability disclosure policies setting out how vulnerability reports will be received and handled, what the reports should contain, approaches for disclosure to affected users and the public, as well as any rewards policies.

The **Responsible Disclosure Guidelines** below set-out in greater detail how SingCERT, Informers, and System Owner(s) can contribute to the RVD process, and actions to adopt or avoid. By voluntarily submitting a vulnerability report to SingCERT, the Informer agrees to be bound by the terms stated in this vulnerability disclosure policy. System Owners will be required to acknowledge and agree to this vulnerability disclosure policy prior to receiving information from SingCERT.

Please note that nothing in this Policy or the Responsible Disclosure Guidelines authorises or permits the taking of any action which may contravene any applicable laws (including the Singapore Computer Misuse Act 1993, Personal Data Protection Act 2012, or any applicable foreign laws). Informers are reminded to abide by all applicable laws, including when taking any steps to identify or verify the vulnerability. Reporting a vulnerability to SingCERT under this policy does not exempt any person from applicable laws, and does not preclude or confer any protection from legal liability or investigations by relevant law enforcement agencies.

Reporting of Vulnerabilities in the Singapore Government Systems or Infrastructure

For reporting of vulnerabilities in the Singapore Government's systems or infrastructure, please report it to Govtech at https://www.tech.gov.sg/report_vulnerability

Responsible Disclosure Guidelines

In this section, we outline the roles that Informers, System Owner(s), and SingCERT may play in the RVD process. The guidance provided in here is not exhaustive, and may not always be applicable in your situation. Readers are encouraged to consider how the guidance provided here may be applied to their specific circumstances, and seek professional legal advice where required.

Informers should:

1. Always act responsibly, with good faith and exercising reasonable care, for the sole purpose of reporting suspected vulnerabilities to System Owner(s) to help ensure a safer cyberspace. Where possible, the System Owner(s) permission should be obtained before performing any actions, especially actions that may adversely affect System Owner(s) and users. Where possible, SingCERT aims to have the Informers work with System Owner(s) to resolve any validated vulnerability within 90 working days, subject to any agreement or arrangement between them. Informers should also refrain from disclosing information about the vulnerability to any third parties or the public before System Owner(s) have had sufficient time to develop and implement solutions to mitigate or eliminate the vulnerability. Informers may come across personal, sensitive, and/or confidential information in the course of the RVD process. Informers should ensure that their actions do not compromise the confidentiality of any such information, including by creating unauthorised reproductions of the information or by disclosing the information to unauthorised persons. The Informer agrees that in the event of a dispute between the Informers and System Owner(s), the Systems Owner(s) will have the final decision regarding the disclosure of the reported vulnerability.

2. Be deliberate and take due care when performing actions pertaining to assessing a vulnerability. This includes ensuring that the actions do not cause losses of any kind, do not compromise the availability of systems and services, and avoiding actions that are not strictly necessary for the purposes of assessing, testing, or evaluating the security of the systems and services in order to ensure or safeguard their security. In particular, Informers should not use disruptive or destructive means to find vulnerabilities, including attacks on physical security, social engineering, denial of service, spam, brute force, or third party hacking/scanner applications to target websites.

3. Comply with all applicable Singapore and foreign laws. This includes complying with the Singapore Computer Misuse Act ("**CMA**") and refraining from actions that may constitute a breach of the CMA. You are advised to seek and obtain professional legal advice if you have any doubt about the scope and application of any law. Some illustrative, non-exhaustive examples of actions which Informers should not take include:

a. Gaining unauthorised access to computer system(s) and establishing persistent access, or disrupting any computer process or service. Examples: Deploying trojan-downloaders to install backdoors or installing virus or malicious malware

b. Modifying the contents or configuration of any computer system(s), causing disruption or degradation to the system. Examples: Altering IT configurations/parameters to disrupt the system, or deploying malicious software into the system

c. Accessing or modifying the memory or data of any computer system where not strictly necessary for the purposes of assessing, testing, or evaluating the security of the system or service. Examples: Changing portions of a webpage or deleting database entries

d. Intercepting a computer service where not strictly necessary for the purposes of assessing, testing, or evaluating the security of the service. Examples: Using network interception or browser proxy tools to intercept network traffic, to steal session cookies, or to modify another user's session cookie, hampering others from using the service

e. Obstructing the use of computer systems, or preventing others from accessing any program or data stored in the system. Examples: Causing a denial-of-service on the computer systems, or preventing other users from accessing them

f. Unauthorised access to and disclosure of passwords, access codes, or any other means of accessing a computer system. Examples: Publishing credentials on the Dark Web or other forums

g. Obtaining personal or corporate information and using that material to commit illegal activity. Examples: Harvesting and exfiltrating business data for monetary gains, fraud or blackmail

h. Deploying disruptive or unlawful means to detect vulnerabilities. Examples: Attacks on physical security, social engineering, denial of service, brute force attacks

i. Carrying out attempts or preparatory acts to do any of the actions listed at 3(a) to (h) above

4. Provide adequate information on the reported vulnerability and work with the System Owner(s) to validate the suspected vulnerability, including these details (where available):

a. Description of the suspected vulnerability

b. Product(s)/service(s) affected, along with the model or software versions

c. IP address and/or URL of the subject service (if applicable)

d. Description of the methods and circumstances, including date(s) and time(s), leading to your discovery of the suspected vulnerability

e. Description of the reason(s) why you believe the suspected vulnerability may impact the subject product/service and the extent of potential impact (e.g. describe how you believe the suspected vulnerability might potentially be exploited). You may also include the Common Vulnerability Scoring System (CVSS) calculations, possible attack scenarios, or required conditions for exploitation

f. Any other relevant information such as network packet captures, crash reports, video recording or screenshots providing evidence of codes or commands that were used in the discovery of the suspected vulnerability

5. Provide your name, email, and contact number in the vulnerability report. System Owner(s), SingCERT, or law enforcement agencies (e.g. the Singapore Police) may contact you for further clarifications, or to seek your assistance in investigations relating to the vulnerability and any actions you may have taken in the course of the RVD.

6. Specify in the vulnerability report whether the System Owner(s) have been notified or if there is a plan to inform the System Owner(s) about the vulnerability.

System Owner(s) should:

1. Conduct its own verification and assessments on any information regarding a suspected vulnerability. This includes the potential impact of exploitation.

2. Contact the Informer, while keeping SingCERT informed, if more information on the suspected vulnerability is required, and work with the Informer in providing a simultaneous public disclosure, if appropriate.

3. If the suspected vulnerability is verified, Systems Owner(s) should:

a. Work towards developing a patch, workaround, or mitigation measures

b. Ensure that product/service users are aware of the vulnerability and the appropriate mitigation measures. This may be in the form of notifications to the affected users, or the publishing of an advisory. Where appropriate, System Owner(s) should notify product/service users of interim mitigations (if any) while the patch is being developed, to minimise damage or harm to individuals and organisations as malicious actors may also discover and exploit the vulnerability

c. Update SingCERT and the Informer of its assessments, findings, and status on the response to the vulnerability

Subject to the terms of this policy,

SingCERT will:

1. Act as a conduit to coordinate between the Informer and System Owner(s), if deemed appropriate.

2. If deemed appropriate, assign a CVE ID to the newly identified cybersecurity vulnerability if it is not within the scope of another CVE Numbering Authority (CNA). This should be done within 14 working days after the System Owner(s) verify and consent to its public disclosure.

3. Make reasonable effort to contact the System Owner(s) as soon as practical after receiving a vulnerability report. Where necessary and appropriate, we may put the Informer and System Owner(s) directly in touch, or provide the Informer's name and contact details to the System Owner(s), to enable better communication and coordination.

4. Assist in any investigations, including those by law enforcement agencies.

5. Where circumstances warrant, we reserve the right, at any point in time, to:

   a. Reject, redirect or prioritise any vulnerability reports received, or

   b. Cease to act as coordinator between the Informer and the System Owner(s)

6. Disclose an advisory about the vulnerability associated with the assigned CVE ID on CSA's website when the coordination is completed, which happens when the System Owner(s) release a patch, workaround, or mitigation measures.

SingCERT will NOT:

1. Verify or conduct technical analysis on the information provided by the Informer before conveying it to the System Owner(s).

2. Be obliged to consult you for any public statements that we or the System Owner(s) considers necessary to release.

3. Provide any reward or incentive such as a 'bug bounty'.

4. Accept any liability to the Informer, the System Owner(s), or any other party for any direct or indirect loss or damage of any kind.

5. Pursue legal action on behalf of another party.

6. Condone any breach of the law, including the Computer Misuse Act or Personal Data Protection Act.

7. Provide the Informer with any protection from civil or criminal liability, or excuse the Informer from having to assist in any investigations.

8. Handle under this Policy complaints, feedback, or other information on issues that do not relate specifically to cybersecurity vulnerabilities in products or services. This includes information provided by whistle-blowers on potential wrongdoing.

9. Make any express or implied representation or warranty regarding the suspected vulnerability report or its accuracy. Also, the coordination of the report does not constitute any endorsement, verification, or recommendation by SingCERT.

Reporting a Vulnerability to SingCERT

For reporting of a suspected vulnerability, please submit the Vulnerability Reporting Form at https://go.gov.sg/vulnreport or email us at SINGCERT@csa.gov.sg. For any sensitive data and information, please use PGP encryption. Our PGP public key can be found below. For more information on how to perform PGP encryption, please refer to https://www.openpgp.org/software/.

Download PGP Key

SingCERT will send you an acknowledgement receipt within 5 business days, along with further details on the process if deemed necessary.

SingCERT reserves the right to accept, reject, or prioritise any vulnerability report at its discretion. The decision to accept or reject the vulnerability disclosure coordination role for a particular disclosure will generally be based on the scope and severity of the vulnerability and our ability to resource the process.

In cases where the System Owner(s) is unresponsive, does not agree with the Informer's vulnerability report, or stop responding to coordination requests, SingCERT may consider closing the report within 120 days after the initial attempt to contact the System Owner(s). If the Informer request to continue coordination, SingCERT reserves the right to decline such requests.

SingCERT may consider a report invalid if:

1. The issue has limited security impact and/or is a known issue.

2. The Informer is uncontactable for further information required or refuses for any reason to release further information.

or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.