Factsheet on Government Crowdsourced Vulnerability Discovery Programmes

The Government Technology Agency (GovTech) is the public sector lead that safeguards the Singapore Government's Infocomm Technology and Smart Systems (ICT & SS) and enables Singapore to be a safe and secure Smart Nation.

As part of the Government's ongoing efforts to strengthen the security posture of our ICT systems and digital services used by citizens, businesses and public sector employees, GovTech works closely with the global cybersecurity researcher community and members of the public to augment the government's cybersecurity capabilities.

GovTech runs three crowdsourced vulnerability discovery programmes:

Programme	**[NEW] Vulnerability Rewards Programme (VRP)**	**Government Bug Bounty Programme (GBBP)**	**Vulnerability Disclosure Programme (VDP)**
Mode of operation	Continuous	Seasonal	Continuous
Systems	Selected internet-facing critical systems	5 to 10 selected critical and other high-profile systems in each iteration	All internet-facing systems
Who can participate	All registered HackerOne 'white hat' hackers who have achieved HackerOne Clear status and invited local 'white hat' hackers	Only invited highly-skilled 'white hat' hackers	Any member of the public
Reward	Monetary reward	Monetary reward	HackerOne reputation points

[NEW] Vulnerability Rewards Programme

The Vulnerability Rewards Programme (VRP) is a new crowdsourced programme that rewards 'white hat' hackers who discover vulnerabilities in critical government systems.

The programme will first start with three systems: Singpass and Corppass (GovTech); Member e-Services (Ministry of Manpower – Central Provident Fund Board); and Workpass Integrated System 2 (Ministry of Manpower). More systems will be progressively added to the programme.

Rewards can range from US$250 to US$5,000 depending on the severity of the discovered vulnerabilities. A special bounty of up to US$150,000 is offered for critical vulnerabilities that could cause exceptional impact on selected systems and data, highlighting the Singapore government's commitment to secure critical government systems and valuable personal data. The special bounty was benchmarked against crowdsourced vulnerability disclosure programmes from leading technology companies[1].

[1] https://security.googleblog.com/2021/02/vulnerability-reward-program-2020-year.html,
https://www.microsoft.com/en-us/msrc/bounty,
https://msrc-blog.microsoft.com/2020/08/04/microsoft-bug-bounty-programs-year-in-review/

To qualify for the special bounty, the vulnerability must minimally:

1) Be classified at the Critical severity level (9.0-10.0), based on the Common Vulnerability Scoring System (CVSS) v3.0 Ratings[2]; and
2) Fall within any one of the Exceptional Impact Categories specified in the VRP rules

For more details, please visit https://hackerone.com/govtech-vrp.

Government Bug Bounty Programme

Launched in Dec 2018, the Government Bug Bounty Programme (GBBP) is a seasonal programme that invites highly-skilled 'white hat' hackers – or ethical hackers – to conduct in-depth testing of selected systems to discover vulnerabilities in ICT systems. Bounties are paid for valid vulnerabilities depending on the severity of the discovered 'bug', and the discovered 'bug' will subsequently be reported to the respective agency for remediation.

As of August 2021, there have been four iterations of the programme, covering a total of 33 systems. Each iteration ran for a period of two to three weeks and involved five to 10 selected systems. The selected systems comprised Critical and other high-profile systems that have high user touchpoint.

More than 1,000 local and international 'white hat' hackers have participated in the four GBBP iterations. In total, over 100 valid vulnerabilities have been reported and promptly remediated, with more than US$100,000 paid out to the participants.

GovTech will continue to conduct the GBBP several times a year, signaling the Government's continued commitment to work with the global cybersecurity community and industry to strengthen and safeguard government ICT systems and digital services.

Vulnerability Disclosure Programme

The Vulnerability Disclosure Programme (VDP), launched in October 2019, invites members of public to report vulnerabilities found in any Government Internet-facing web-based and mobile applications. Validated vulnerabilities under the VDP will be rewarded with HackerOne reputation points

The VDP serves as an evergreen crowdsourcing platform to encourage responsible reporting of any suspected vulnerability, while strengthening the public's sense of collective ownership over the cybersecurity of Government systems.

As of March 2021, over 900 vulnerabilities from 59 agencies have been reported; more than 400 reports were valid vulnerabilities which were promptly remediated.

Members of the public can report a suspected vulnerability in two ways:

i. Use the vulnerability disclosure link ("Report Vulnerability") incorporated into all Government webpages and mobile applications
ii. Email vulnerability_disclosure@tech.gov.sg with details of the suspected vulnerability

For more details, please visit https://www.tech.gov.sg/report_vulnerability.

[2] Refer to the CVSS table at https://nvd.nist.gov/vuln-metrics/cvss