Factsheet about 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	Vulnerability Rewards Programme (VRP)	Government Bug Bounty Programme (GBBP)	Vulnerability Disclosure Programme (VDP)
Year of Launch	2021	2018	2019
Mode of operation	Runs all year round	Two to four times a year; two weeks per run	Runs all year round
Systems	Internet-facing critical systems	Five to 10 selected critical and other high-profile systems in each iteration	All Internet-facing systems
Who can participate	All registered YesWeHack researchers who are highly skilled and have been KYC-Verified, and invited local researchers	Only invited highly skilled researchers	Any members of the public
Reward	Monetary reward	Monetary reward	Ranking points

Vulnerability Rewards Programme

The Vulnerability Rewards Programme (VRP) is a crowdsourced programme that rewards researchers who discover vulnerabilities in critical government systems.

The programme started 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). As of February 2023, 20 more systems were 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].

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

[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/

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

As of February 2024, more than 400 local and international researchers have participated in the programme. In total, 27 valid vulnerabilities have been reported and promptly remediated.

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

Government Bug Bounty Programme

The Government Bug Bounty Programme (GBBP) is a seasonal programme that invites highly skilled researchers – or ethical hackers – to conduct in-depth testing of selected ICT systems to discover vulnerabilities in them. 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 February 2024, there have been eleven iterations of the programme, covering a total of 82 systems. Each iteration ran for a period of two weeks and involved 5 to 10 selected systems. The selected systems comprised Critical and other high-profile systems that have high user touchpoint.

More than 1,700 local and international researchers have participated in the eleven GBBP iterations. In total, over 200 valid vulnerabilities were reported and promptly remediated, with more than US$150,000 paid out to the participants.

GovTech will continue to conduct the GBBP several times a year, signalling 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) invites members of the public to report vulnerabilities found in any Government Internet-facing web-based and mobile applications. Vaidated vulnerabilities under the VDP will be rewarded with ranking 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 February 2024, over 1,000 vulnerabilities from 129 agencies were reported, with more than 800 reports identified as valid vulnerabilities and promptly remediated.

Members of the public can report a suspected vulnerability through the vulnerability disclosure link ("Report Vulnerability") found on all Government websites and mobile applications.

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