BIGO Bug Bounty Program Policy

By participating in the program, you agree that you are bound by and subject to this policy. We may modify the terms of this policy or terminate the policy at any time.

If you do not comply with this policy or if we determine that your participation in the program is not in good faith or could adversely impact us, our affiliates, or our business partners (or any of our or their users, employees, or contractors, we, in our sole discretion, may remove you from the program and disqualify you from receiving any reward under the program).

In this Policy, unless otherwise provided in this Policy, the following term has the same meaning as follows:

Whitehat refers to the abbreviation of the reporter who submits vulnerability and threat intelligence in this plan

Response Targets

Processing stage

- Time to first response (from successful report submission): 1 business day

- Time to triage (from successful report submission): 3 business day
- Time to bounty (from triage): 5 business days

Depending on the complexity of the report and our current report flow, we may take longer to respond. We'll try to keep you informed about our progress throughout the process.

Program Rules and Guidelines

- Provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.
- Submit one vulnerability per report unless you need to chain vulnerabilities to provide impact.
- If more than one person reports the same security vulnerability, the reward will generally be given to the first person to successfully submit the report. Exceptions may be made case by case.
- Multiple vulnerabilities caused by one underlying issue may be awarded one bounty.
- Social engineering of any kind (including without limitation phishing, vishing, smishing) is prohibited.
- Do not commit privacy violations, destruction of data, or interruption or degradation of our service. Create test accounts or test content to avoid

affecting real users; do not test vulnerabilities on user accounts that you do not own or have rights to access or control.

- Do not exploit vulnerabilities beyond a good faith effort to test the issue.

Core business

The following are core businesses:

- Hello Yo
- Imo
- Bigo Live
- Likee

Disclosure and Confidentiality Policy

Before receiving the express written authorization from our company, please do not publicly disclose or provide any detailed information about the safety breakthroughs of our products or services, and do not conduct any breakthrough transparent hype and public relations.

Vulnerabilities Rewards

BIGO may, at its discretion, provide rewards to qualified whitehat of qualified vulnerabilities. Rewards are usually paid in the following month. Whitehat shall issue a legal and valid invoice before BIGO makes the payment. The bank transfer fees which is chargeable as per the Bank's process and guidelines shall be borne by BIGO. The following table outlines the nominal rewards for specific categories of vulnerabilities for the attributes in the scope (see the "Scope" section).

The amount paid by BIGO to the whitehat under this Policy shall be inclusive of all applicable taxes, including but not limited to income tax, value added tax, wit hholding tax, sales tax or any other related taxes imposed by authorities in the T erritory.

The whitehat shall be responsible for declaration and payment of all applicable t axes mentioned above in the manner being prescribed by law.

Rewards in USD

Vulnerability hazard business type	Critical	High	Medium	Low	No impact
Core Business	700～1200	380-700	70-230	0-30	0

General business	230-460	70-230	30-70	0-15	0

【Critical】

1. Vulnerabilites that permit directly talking over BIGO servers.

2. Vulnerabilites that permit in leakage of highly user-sensitive plldata of core products. or that affect the security of users'identity information.

3. Vulnerabilites that permit sending messages to other users via spoofed BIGO id, or that permit resetting passwords of other user's account.

【High】

1. Affect a certain range of user account or fund security, including but not limited to: non-core DBSQL injection, storage type XSS that can cause automatic propagation, CSRF involving transactions, funds, and passwords, which can lead to user account security application system vulnerabilities or Business logic defects, etc.

2. Sensitive information leakage includes but is not limited to non-core DB SQL injection, source code compression package leakage, server application encryption reversible or plaintext, mobile API access summary, hard coding and other issues caused by sensitive information interference.

3. A wide range of other defenses that affect users. Including but not limited to storage type XSS (including storage type DOM-XSS) of important pages that can cause automatic transmission and CSRF involving transactions, funds, and passwords.

【Medium】

1. Vulnerabilities that require interaction to affect users. Including but not limited to storage XSS for general pages, including but not limited to storage XSS for general pages, JSONP hijacking of sensitive information, and CSRF for important operations.

2. Ordinary unauthorized operations include, but are not limited to, incorrect direct object references, broadcast message forgery that affects business operations, and other Android component permissions vulnerabilities.

3. Common information leakage Including but not limited to client plaintext storage password, client password plaintext transmission, web path traversal, system path traversal.

4. Remote denial of service vulnerabilities include, but are not limited to, remote denial of service on the client side (parse file format, network protocol crashes), problems caused by the exposure of Android component permissions, and common application permissions (under the default configuration).

5. Hijacking of subdomains in the business scope.

6. OAuth login or binding hijacking that needs to click on the link to interact.

【Low】

1. Vulnerabilities that can be executed only in specific browsers (such as lower than IE 11) or client environments and have less impact, including but not limited to reflective XSS, non-critical business storage XSS, etc.

2. It is difficult to use but there may be safety hazards. Including but not limited to

Self-XSS that may cause dissemination and exploitation, CSRF for non-critical sensitive operations, SMS bombs, brute force cracking without guessing user passwords, and JSONP vulnerabilities.

3. Low-sensitivity information leakage includes, but is not limited to, path leakage, non-core code SVN file leakage, non-sensitive system source code and passwords leaked by phpinfo and GitHub, etc.

4. Vulnerabilities that are being repaired based on official alerts of equipment, systems, software or frameworks.

5. Reflective XSS needs to obtain user-sensitive cookies, if only alert (document.domain) may not make much sense.

【No impact】

1. Network security bugs, including but not limited to garbled webpages, webpages cannot be opened, and certain functions cannot be used.

2. Unexploitable "vulnerabilities". Including but not limited to scanner vulnerability reports that have no practical significance (such as the low version of Web Server, etc.), Self-XSS, JSON hijacking without sensitive information, sensitive and non-operational CSRF, meaningless source code leakage, intranet IP address/ Domain name leakage, 401 basic authentication phishing, program path trust issues, and logcat information leakage without sensitive information. The use of vulnerability scanners to scan servers/businesses is prohibited.

3. Without any precautions. Including, but not limited to, your account is stolen, it

means there is a loophole.

4. Prohibit sending phishing emails to BIGO internal employees

Threat intelligence Rewards

BIGO may, at its discretion, provide rewards to qualified whitehats of qualified threat intelligence. Rewards are usually paid in the following month. Whitehats shall issue a legal and valid invoice before BIGO makes the payment. The bank transfer fees which is chargeable as per the Bank’s process and guidelines shall be borne by BIGO. The following table outlines the nominal rewards for specific categories of threat intelligence for the attributes in the scope (see the "Scope" section).

Rewards in USD

Threat level	Critical	High	Medium	Low	No impact
Complete	920	300～460	76～153	7~46	0
Incomplete	150~230	50~100	15~46	0~7	0

Threat Intelligence Scoring Rules:

Threat intelligence scoring is given by BIGO SRC with comprehensive factors such as business level, actual impact and intelligence clues integrity. According to the degree of intelligence hazard, the intelligence level is divided into five levels: [Critical], [High], [Medium], [Low], and [No impact].

【Critical】

1. The core business server was invaded and related behavior characteristics were provided to facilitate rapid location and confirmation of problem points.
2. The core business database is dragged and provided with clues such as the database name or database file, time correlation, etc.
3. Major 0Day vulnerability. Such as undisclosed or semi-disclosed vulnerabilities in core server software and systems, undisclosed or semi-disclosed vulnerabilities in core office software, etc.
4. Intelligence of threat organization activities that have a significant impact on core business. Such as large-scale theft of BIGO core business accounts.

【High】

1. Intrusion clues of non-core business systems.
2. Threat organization activity intelligence that has a greater impact on core business, such as DDoS intelligence, etc.
3. New viruses, Trojan horses, and worms that can cause major impacts. Such as large-scale worm incidents caused by storage XSS vulnerabilities in important businesses.

【Medium】

1. New available tools and methods. Such as: tools that can scan account numbers by bypassing the strategy; (tools need to provide attack principles and repair solutions for reference.)

2. Medium risk business security issues, such as cheating activities and bypassing business rules;

3. The basic information of the threat organization, including but not limited to the threat organization related personnel, structure, scale, region, activities and other information, communication and sales channels, tools and platforms used, related impacts, industry trends, etc.;

【Low】

1. Low-risk business security issues. Such as malicious registration, commenting, etc.;

2. Phishing websites that fake BIGO business, etc.

【No impact】

1. False or invalid information that cannot be verified or artificially created.

2. Known information inside BIGO, etc.

3. Unable to restore report intelligence information or fail to provide valid information, etc.

The following issues are outside the scope of our vulnerability rewards program (either ineligible or false positives):

- Attacks requiring physical access to a user's device
- Any physical attacks against BIGO property or data centers
- Forms missing CSRF tokens (we require evidence of actual CSRF vulnerability)
- Logout CSRF
- Password and account recovery policies, such as reset link expiration or password complexity
- Invalid or missing SPF (Sender Policy Framework) records
- Content spoofing / text injection
- Issues related to software or protocols not under BIGO control
- Reports of spam (see here for more info)
- Bypass of URL malware detection
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
- You are the member, consultant or employee of BIGO
- Issues without clearly identified security impact, such as clickjacking on a static website, missing security headers, or descriptive error messages
- Issues that result in Denial of Service (DoS) to BIGO's servers at the network or application layer.
- If you believe your account has been compromised, please contact BIGO support

directly.

The decision to grant a monetary rewarded and the final amount for a vulnerability will be within the discretion of the BIGO Security Team.

Good Faith Guidelines

To the extent your security research activities are inconsistent with certain restrictions in our relevant site policies but are consistent with the terms of our bug bounty program, we may waive those restrictions for the sole and limited purpose of permitting good faith security research under this bug bounty program.

If your security research involves the networks, systems, information, applications, products, or services of a third party, including any BIGO users, we cannot bind that third party, and they may pursue legal action or law enforcement notice. We cannot, and do not, authorize security research in the name of other entities or individuals, and cannot in any way offer to defend, indemnify, or otherwise protect you from any third party action based on your actions.

You must, as always, comply with all laws applicable to you, and not to disrupt or compromise any data beyond what our bug bounty program permits.

Contact us before engaging in conduct that may be inconsistent with, or unaddressed by, this policy. Be proactive in contacting us before engaging in any action that may violate this policy or good faith.