Community Rules v6.0

Last Update：2021.5.17

Collection Agreement

To standardize the DVP community vulnerability collection procedure, BCSEC and PeckShield wrote this agreement to build the community consensus at the early stage. The agreement will keep updating according to community feedbacks.

Collection Range

Type A Vendors： Members of the bounty program. The claim of vulnerabilities directly depends on the vendors.

Type B Vendors: Non-members of the bounty program. Type B vendors have blockchain related products，including but not limited to exchanges, cryptocurrencies, software and hardware. DVP would temporarily claim valid vulnerabilities for first-class vendors if we fail to contact the vendors to claim in time. Rewards for other unclaimed Type B Vendors' vulnerabilities shall be distributed according to the class-four vendors standard. Note： Type B vendors are not fixed, as they may be changed to Type C in some cases

Type C vendors :Non-relevant vendors. Vendors that DVP has defined as irrelevant, including but not limited to information sites(such as market trend alerts), and e-commerce websites (such as websites that sell mining machines), which are not directly relevant to blockchain or cryptocurrency,or projects out of normal operations (such as abandoned projects, scam, etc.)

Explanation for Type A Vendors

If a Type A vendor cannot be reached, or fail to give an effective response to the vulnerability submission, DVP will use the bounty pool reserved by the vendor to reward the white hat. If the bounty pool is insufficient, DVP will suspend the vulnerability recording of this vendor.

If there's not doubt about the impact of the vulnerability but controversy about the bounty amount, DVP will reward the white hat with bounties the vendor reserved before, according to the registered vendors' bounty plan, after failing to negotiate for couple of times. If the bounty pool is insufficient to pay the rewards for the white hat, DVP will provide appropriate subsidizes and remove the vendor. Explanation for Type B Vendors

The following reward standards are for Type B vendors，The rewards is ultimately decided by the actual impacts of the vulnerability. When the actual impact is lower than the vulnerability itself demotion rule will be activated.

All vulnerabilities or threat intelligence must satisfy three conditions: Not published, not fixed, and not submitted to other platform.

If the target type is not in the reward range (such as tokens, exchanges, mainnet，etc.), but the target is somewhat important in the blockchain industry, please submit it as a threat intelligence first, and the reward would be assessed according to the vulnerability's actual impacts.

DVP does not speculate about any vulnerability, and all evidence about the vulnerability needs to be presented clearly in the vulnerability report. DVP does not accept vulnerabilities that are only theoretically valid.

If the vulnerability belongs to the non-main business of the vendor, please refer to the Non-core Vulnerability Rules for the corresponding reward.

For vulnerabilities that do have some impacts but not covered by the reward rules, or the rules are not fair enough, we will improve according to community feedbacks. This is version 4.0, and it will continue to be iterate based on community feedback.

Vulnerability rewards are valued according to the actual impact of vulnerabilities. The following reward tables shows the highest possible reward of one vulnerability of specific severity level and vendor level, and the unit is USDT.

DVP has defined the level of the targets and level of the vulnerability, so when submit vulnerability reports, please correctly select the levels and related links for the review. if the information is false and misleading, DVP will record the behavior and severely punish the submitter.

If vulnerability/threat intelligence cannot be classified by this agreement, then would be assessed according to CVSS vulnerability classification standard.

When submitting the vulnerability report, please attach a screenshot of the vendor's ranking at the time of submission, and also make sure to include the date and time in the same screenshot as well. During auditing, DVP will firstly check the authenticity of the information in the screenshot, and if the information is true, DVP will use rewards standards according the ranking in the screenshot. But if the information is false and misleading, DVP will severely punish the submitter. If there are no screenshot about ranking in the report, DVP will use the rankings which was seen when DVP audits.

It is highly recommended to submit vendor's contact to facilitate the communication if the vendor hasn't taken part in the bounty program.

Reward Criterion

Exchanges

	High Risk	Medium Risk	Low Risk
Level 1(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200

Level 3(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(DVP)	1000	500	200

Level classification data：https://www.coingecko.com/en/exchanges

Level 1 List:

Binance	Huobi	FTX	OKEX
Bithumb	UPBIT	CoinBase	BFX
Bitstamp	Bitflyer	Gemini	Upbit
BitMEX	Bitfinex	Kraken	Bakkt
Bybit	BitMex		

Level 2：Exchanges ranking in the top 20 on Coingecko, except for the list of Level 1 exchanges in the above table.Coingecko （If the exchanges in Level 2 decide to reward the white hats more than the standards present here, DVP will give the extra rewards to the white hat without reserve）

Level 3：ExRank top 40

Level 4：ExRank lower than the top 40

High risk：Need proof of real exploitation, not issues only in theory.

• Can directly get system privilege;

• Severe design fault/logic vulnerability related to key business;

• Affect user/company assets, including but not limited to severe payment vulnerability, and digital asset private key leaks;

• Can lead to market manipulation, such as illegal operations that initiate buy/sell trades;

• Can directly get backend access privilege;

• Can directly get large amount of sensitive information, including but not limited to source code, and SQL injection;

• Can directly, without interaction, steal large amount of users or backend admin IDs, including but not limited to user visible page storage type XSS, and backend visible XSS (Need proof that can access backend information, otherwise would be classified as medium or low risk);

Medium risk: Need proof of real exploitation, not issues only in theory.
• Some sensitive information leaks, including but not limited to SSRF internal network information leaks, and partial user information leaks;

• Need ways like interaction and explosion to steal user IDs, including but not limited to non-typical page storage type XSS and backend invisible XSS;

Low risk: No proof of real exploitation, but issues in theory
• Non-Sensitive information exposure, including but not limited to directory traverse;

• Other vulnerabilities where there is no proof of real exploitation, but issues in theory;

Vulnerabilities are not accepted for the time being(not including Bounty Vendors):
• SPF mail forge vulnerabilities

• Vulnerability steal user account name using Interface exhaust explosion

• Self-xss/Post type XSS vulnerabilities that cannot be exploited

• Vulnerabilities of identity theft with high interaction requirements, including but not limited to reflective XSS and general CSRF

• URL jumping vulnerability

• Text message interface abuse issues, etc.

• Vulnerability of Denial of Service

• Mail explosion

• Vulnerabilities whose vendor is not in normal operation (abandoned projects, Ponzi scheme projects, etc).

• Vulnerabilities whose vendor is not in normal operation (abandoned projects, Ponzi scheme projects, etc).

• Design fault/logic vulnerability that only affect own account

Blockchains/Cryptocurrencies

	High Risk	Medium Risk	Low Risk
Level 1(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
Level 3(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(DVP)	1000	500	200

Level classification data：https://coinmarketcap.com

Level 1: Market cap top 10

Level 2: Market cap top 20

Level 3： Market cap top 40

Level 4： Market cap below top 40

Severe: Need proof of real exploitation, not issues only in theory

• Can remotely get access privilege;

• Can directly steal digital assets;

• Severe sensitive information leaks, including but not limited to user private keys and passwords;

High risk: Need proof of real exploitation, not issues only in theory;

• Can lead to denial of services;

• Design flaws/logic vulnerablities that affect large amount of users/exchanges;

• Can destroy or re-issue digital assets unconditionally;

• Can lead to unconditional denial of services of the key functions of smart contract;

Medium risk: Need proof of real exploitation, not issues only in theory;

• Can lead to local privilege upgrade;

• Design flaws/logic vulnerabilities that affect user's own account;

• May lead to high risk vulnerabilities indirectly;

• Can destroy or re-issue assets to some users under some conditions;

• Can steal contracts or contract users' digital assets under some conditions.

Low Risk：

• General information leaks;

• Low impact design flaws/logic vulnerabilities;

• Can cause system resource abuse or user spam;

• Other vulnerabilities where there is no proof of real exploitation, but valid in theory, including but not limited to the bugs that only could be exploited by the owner.

Wallets

	High Risk	Medium Risk	Low Risk
Level 1(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
Level 3(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(DVP)	1000	500	200

Level classification data: https://www.feixiaohao.com/wallet/

Level 1 Wallets List：

TP	imToken	Math	Cobo

Trust	Metamask		

Level 2：Ranking top 10 except the wallets in the above list;

Level 3：Ranking top 20

Level 4：Ranking below top 20

High risk: Need proof of real exploitation, not issues only in theory.

• Can remotely get service/client access privileges unconditionally

• Can lead to stealing of large amount of digital assets unconditionally;

• Can lead to severe sensitive information leaks unconditionally, including but not limited to user private keys, passwords, etc.

• Can unconditionally lead to large amount of sensitive information leaks;

• Can unconditionally lead to service/client denial of services;

• Can unconditionally lead to stealing of large amount of user IDs.

Medium risk: Need proof of real exploitation, not issues only in theory

• Can lead to malicious changes of user information;

• Can lead to small amount of sensitive information leaks;

• Can unconditionally lead to stealing of small amount of user IDs;

Low risk:
General information exposure;

• Non essential business design flaws/logic vulnerabilities;

• Non essential business design flaws/logic vulnerabilities;

Mining pools

	High Risk	Medium Risk	Low Risk

Level 1(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
Level 3(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(DVP)	1000	500	200

Level Classification data from:https://btc.com/stats/pool?pool_mode=year

Level 1 Mining Pool List:

F2Pool	Binance Pool	Huobi.pool	AntPool
Spark pool			

Level 2: top 10

Level 3: top 15

Level 4: Not in top 15 but still in the ranking list

Severe: Need proof of real exploitation, not issues only in theory

• Can unconditionally remotely get mining pool all privileges;

• Can unconditionally remotely control all mining pool computation power;

• Can unconditionally steal mining pool reward or wallet money;

• Can unconditionally lead to denial of services of mining pool's essential business;

• Can unconditionally lead to mining pool interest loss, such as block withholding attacks, forge computing power, etc;

• Can unconditionally lead to large amount of sensitive information leaks.

Medium risk: Need proof of real exploitation, not issues only in theory

• Design flaws/logic vulnerabilities that can lead to some risk.

Low risk:

• Can lead to small amount of information leaks

• Can have real impact under specific conditions

DEFI

	High Risk	Medium Risk	Low Risk
Level 1(ETH)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(ETH)	1500 ~ 2500	250 ~ 1000	50 ~ 200
Level 3(ETH)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(ETH+DVP)	1000	500	200

Level classification data from:https://www.coingecko.com/en/defi（7-day trading volume）

Level 1: top 10

Level 2: top 50

Level 3: top 200

Level 4: below top 200

High risk:

• Can unconditionally steal contracts or contract users' digital assets

• Can unconditionally destroy or re-issue digital assets;

• Can unconditionally lead to denial of services of contracts' important functions.

Medium risk:

• Can create or destroy some users' digital assets;
• Can steal limited contracts or contract users' digital assets.

Low risk:

• Other vulnerabilities where there is no proof of real exploitation, but valid in theory, including but not limited to the bugs that only could be exploited by the owner.

Threat Intelligence

	High Risk	Medium Risk	Low Risk
Level 1(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
Level 2(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
Level 3(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
Level 4(USDT)	1000	500	200

High risk:
• Concrete proof of large amount of blockchain related sensitive information leaks;

• Concrete proof of stealing of large amount of non-personal digital assets;

• Concrete proof of exploitation of unpublished severe blockchain related vulnerabilities;

• Concrete proof of invasion of well-known blockchain related vendors;

• Concrete proof of large scale attacks to blockchain related industry;

• Concrete proof of existence of backdoor in blockchain related hardware/software;

• New attack approaches to blockchain related industry;

Medium risk:
• Clues of exploitation of blockchain related vulnerabilities;

• Clues of unpublished hot blockchain related security events;

• Sensitive information leaks of blockchain related vendors.

Low Risk：
• Clues of exploitation of blockchain related vulnerabilities;

• Clues of unpublished hot blockchain related security events;

• Sensitive information leaks of blockchain related vendors.

Low risk:

• Blockchain related fake websites or apps, etc;

• Clues of attacks against blockchain related industry.

Non-core Vulnerability Rules

Non-core vulnerability refers to the vulnerability related to the non-main business of one blockchain projects.

Examples: Website vulnerabilities of blockchain/cryptocurrencies, wallets and DeFi projects

If the non-core vulnerability can cause severe damage to the main business of one project, and also meet the conditions of reward standards above, it shall be dealt with according to general rules.

	High Risk	Low Risk
Level 1(USDT)	500 ~ 2000	50 ~ 500
Level 2(USDT)	250 ~ 1000	50 ~ 200
Level 3(DVP)	500	100

Level 1: Vendors in the Level 1 classification above;

Level 2: Vendors in the Level 2 classification above;

Level 3 and below: Vendors in the Level 3 or lower level

High risk:

• Need proof of real exploitation, not issues only in theory;

• Can obtain system privilege, and there are many sensitive information (more than 120 pieces);

• Can log in to sensitive database;

• Can log in to sensitive mailbox;

• Can seriously affect users or projects;

Low Risk:

• Need proof of real exploitation, not issues only in theory;

• Storage XSS, need to prove background privilege;

• Can log in to non-sensitive mailbox;

• Can log in to non-primary database;

• A small amount of sensitive information leaks.

Demotion Rules

The final criteria for vulnerability rewards depend on the actual impact of the vulnerability.
The actual impact of a vulnerability is determined by multiple dimensions, including but not limited to the severity of the vulnerability itself, the difficulty of exploiting the vulnerability, the scope of influence, and the actual consequences caused by hackers.

When the actual impact of the vulnerability is lower than the severity of the vulnerability itself, the DVP foundation will downgrade the vulnerability according to the following rules.

Condition for demotion:
Test data in test environment;

Marginalized/abandoned business system;

In the process of vulnerability exploitation, non-ordinary user privileges should be involved, or it's triggered only when certain conditions are met

Multiple weak passwords in the same system;

Other conditions that DVP foundation decide to demote:
A vulnerability demote is at most one level

Example 1: a medium risk vulnerability of a level 2 vendor will be demoted to a low risk vulnerability from of a level 2 vendor.

Example 2: the low risk vulnerability of a level 2 vendor will be demoted to the low risk vulnerability of a level 3 vendor.

General rules

These rules are applied to all vendors except the Bounty Vendors

Vulnerability itself doesn't have value, their value derives from the harm they can bring,so the reward of a vulnerability is decided by vulnerability information submitted by white hats, and its impact range and difficulty of its exploitation.If the triggering condition is very strict, including but not limited to, XSS vulnerability in some specific browsers, the reward level can be adjusted.DVP does not speculate about one vulnerability, and all evidence about the vulnerability needs to be presented clearly in the submitted vulnerability report.

For vulnerabilities not covered by the rewards rules above, DVP may decide to accept them or not.

If one vulnerability can be found among different vendors at least 3 times, then it's regarded as a general vulnerability, after that, more submission would be recorded as repeated submissions, but the vulnerability will be kept for vendors to claim.

The reward targets (such as mainnet, exchange, etc.) in the standard are limited to the vendors themselves. If the submitted vulnerabilities belongs to other assets (including websites and Apps) of the vendors, the demotion rules will be applied according to the actual situation.

To submit a general vulnerability, you must specify the vendor information or provide accurate retrieval syntax, and submit at least five non-abandoned sites as examples.

As for the rewards of general vulnerability, among all the affected vendors, the top three will be rewarded according to the rule, and all the remaining manufacturers will be rewarded according to the average of the top three vendors, that is, the total reward = the reward of top three vendors + (the reward of the top three vendors /3).

Vulnerabilities come from the same source would be counted as one, such as multiple vulnerabilities caused by same interface, multiple page vulnerabilities caused by same publishing system, whole site vulnerability caused by framework , and multiple vulnerabilities caused by pan-domain name resolution; Multiple CSRF vulnerabilities caused by multiple interfaces of the same system exceeding their authority due to the vendor's failure to do identity verification or token verification; Different parameters of the same file, the same parameters appear in different files, the same file in different directories, etc.

These vulnerabilities will not be accepted: interface abuse, SMS explosion, API doc leakage, reflective XSS, DOM-Based XSS, URL jump vulnerabilities, CSRF/JSONP Hijacking/CORS sensitive information with high interaction requirements, and other low risk, high-interaction-required problems.

For storage XSS uploaded to OSS/Bucket, etc., the vulnerability level and rewards will be reduced or rejected directly, depending on the true damage.

Part of the denial of service vulnerabilities (including but not limited to conceptual DoS： for example, frequently sending packages to a certain function causes the slow response of server or denial of service) are not included.

Part of information leakage or design defects of users with high difficulty to exploit will not be accepted.

Vulnerabilities of third-party products include but are not limited to WordPress, Flash plug-ins, server related components such as Apache, OpenSSL and third-party SDK used by enterprises. The same vulnerability in different versions is considered as the same vulnerability.

For the same vulnerability, when the utilization method of later submission has a large impact difference comparing with the utilization method of the first submission, both vulnerabilities are accepted, part of the bonus from the second vulnerability report is allocated to the white hat of the first submission.

The submitted vulnerability details shall not be disclosed or submitted to other platforms, and the violation shall be handled by the DVP arbitration organization by freezing the assets and banning the account.

Vulnerabilities that need to involve non-ordinary user rights during the process of exploiting, or can only be triggered when certain conditions are met, will be downgraded or distribute lower rewards as appropriate.

Vulnerability packaging problem

There are contextual vulnerabilities, such as weak password submitted by the same person into the background, background SQL injection or unauthorized vulnerability merge processing, DVP could consider to improve the level of vulnerability. If has been submitted and later found, then it could be added to the vulnerability, and increase the amount of rewards.

For vulnerabilities that separated submitted, DVP shall review and package the vulnerabilities. The vulnerability level shall be defined according to the highest hazard one in the package, and the rewards shall be paid according to the minimum standard amount. For serious split vulnerabilities, brush vulnerabilities and other malicious behavior, DVP would freeze the account, or even close it. If the following circumstances occur, DVP arbitration organization will freeze the assets of the account.

The latter one of contextual vulnerabilities is submitted firstly. For example: a weak password of mailbox is found and the white hat get the admin password, but the white hat submits the back-end weak password vulnerability first.

Under the excuse of testing the vulnerability, those who take advantage of the vulnerability to harm the interests of users, affect business operations, steal user data, etc., will not be rewarded. Meanwhile, DVP arbitration organization will freeze the assets and close the accounts.

DVP foundation will temporarily reject the vulnerabilities of the type C vendor, and will start to accept the vendor's vulnerabilities again after the vendor meets the requirements. In case of repeated vulnerabilities, the inclusion principle shall be based on the submission sequence after inclusion. Previously rejected vulnerabilities can be resubmitted.

If the vulnerability is not clearly described, it will be rejected directly. For each vulnerability, the URL address, text details, complete screenshot and clear language expression of the vulnerability should be specified, such as:

The vendor must correspond to the domain name, if there is a domain name can not be submitted as IP, additional description requires.

All vulnerability related URLs must be posted at the top of the vulnerability details
The verification steps for vulnerabilities in the proof of vulnerabilities must be detailed to every key operation. In other words, the auditor can completely reproduce the vulnerabilities in accordance with the steps in the proof of vulnerabilities

The payload used in the vulnerability must be posted in text to the details of the vulnerability, not only in the form of screenshots

For marginalized/abandoned business system，demotion will be activated depending on the actual situation

Information leakage vulnerabilities such as github information leakage, memcache, redis and other unauthorized access, etc., will be rated according to the effectiveness and sensitivity of the stored content, while individual information leakage with low harm, such as path leakage, will be ignored.

The front desk hits the storehouse, explodes the kind flaw, must have the successful case proof; Background blasting, only charge successful landing cases, only can blast but no access to the background of the bugs will be rejected.

Weak password problem (normal external registrable system is not included here) :
If the same person finds a different weak password on the same system, it will be consolidated (if the vendor has already processed the previous weak password, it will be consolidated if the second weak password is submitted later).

For the default initial password, only one vulnerability is treated (for example, the initial password of the mailbox is the same password, which is considered as one vulnerability).

For non-key systems, the audit process only confirms the first weak password of the system normally, and the weak password submitted subsequently is ignored.

For key systems or core businesses, only the first two weak passwords are confirmed normally during the rating process, and the subsequent submission of weak passwords is downgraded or ignored.
Do not proceed test that might cause a business to run abnormally, such as an IIS denial of service or a slow_http_dos vulnerability.

For the two vulnerabilities (even though the domain name may be different) of the same interface of the PC and APP, if the same white hat submit them separately, DVP will pack them as one and may increase the rewards accordingly; if different white hats submit them separately, DVP would regard them as duplicates.

For information leakage related vulnerabilities (including GITHUB, when submitting, please specify which features can be proved to be from a certain vendor), can be used in depth to cause great harm, high risk or serious; For the leaks of information such as configuration and code of external core application services, it is generally medium risk; Low risk or rejection treatment if not effective exploitation and non-core business.

Vendor protection

If there are more than three same type vulnerabilities found in one system (such as SQL input or execution etc), auditors may regard the system as no protection, and the same type vulnerabilities submitted later would be demoted.

Conflicts resolution

If there is any disagreement about the vulnerability procedure, level classification, reward, etc, please enter comments into vulnerability detail page or contact online customer service. DVP would coordinate among related parties to resolve conflicts, while giving priority to vulnerability submitters, and may introduce independent security professionals if necessary.

Reference

Some contents are referred from [Xian](#) [Zhi](#) [vulnerablity](#) [classification](#) [standard.](#) Thank you!