DVP Community Rules v5.0

Updated date：2020.04.03

Vulnerability Collection Protocol

To standardize DVP community vulnerability collection procedure, BCSEC and PeckShield wrote this protocol to build community consensus, and this protocol will evolve according to community feedbacks.

Collection Range

Type A vendors: Bounty vendors on DVP, whose vulnerabilities would be claimed by vendors, or not.

Type B vendors: Non-bounty vendors on DVP. They have blockchain related products, including but not limited to, exchanges, cryptocurrencies, software/hardware etc. DVP community would temporarily claim their vulnerablities if the vendors don't come to DVP to claim in time. Caution: **Type B vendors are not fixed, as they may be changed to Type C in some cases**

Type C vendors: Non-relevant vendors. **This types vendors are those that DVP foundation defines as non-relevant**, including but not limited to,

information services, e-commerce websites (such as websites that sells mining machines), etc, which are not relevant to blockchain and cryptocurrency, or which are not in normal operation (abandoned projects, Ponzi scheme projects, etc).

Explanation for Type B Vendors

The following reward standards are for Type B vendors (Type A vendors have customized reward standard).

Reward is not only decided by the severity of the vulnerablity, it's ultimately decided by the actual impacts, taking factors such as exploitation difficulty, affecting range, hackers benefit or not, etc., into account. For example, the reward of one remote command execution bug of a very inactive exchange, would be low accordingly. Demotion Rules will be applied here。

- All vulnerablities or threat intelligence must satisfy three conditions: Not published, not fixed, and not submitted to other platforms.

- If the target type is not in the reward range (tokens, exchanges, public blockchains ...), 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 vulnerablity's actual impacts.

- DVP does not speculate about one vulnerability, and all evidence about the vulnerability needs to be presented clearly in the submitted

vulnerability report . DVP does not accept vulnerabilities that are 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.

- The following reward tables shows the **highest**possible reward of one vulnerability of specific severity level and vendor level.

- We have defined the level of the targets and level of the vulnerabilty, so when submit vulnerablity reports, please correclty select the levels and related links.

- For vulnerablities that have some impacts but not covered by the reward rules, or the rules are not fair enough, we will improve them according to community feedbacks.

- If vulnerablity/threat intelligence cannot be classified by this protocol, they would be assessed according to CVSS vulnerablity classification standard.

Reward standard

Exchanges

	Severe	High risk	Medium risk	Low risk
Level 1(ETH)	31.2	14.4	4.7	0.6
Level 2(ETH)	5.2	2.3	1.0	0.3
Level 3(ETH)	1.6	0.8	0.4	0.2
Level 4(ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
Level 5(DVP)	256	128	64	6

Level classification data from:https://www.feixiaohao.com/exchange/

Level 1：the selected exchanges in the list below

Binance	Huobi Global	Coinbase Pro	OKEX
Bithumb	Gate.io	Bittrex	Poloniex
Bitstamp	Bitflyer	Gemini	Upbit
BitMEX	Bitfinex	Kraken	Bakkt
ZB			

Level 2：ExRank top 50, except the ones in Level 1

(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 80
Level 4: ExRank top 120
Level 5: Not in the top 120 list but has daily trading volume

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

- Can directly get system privilege;
- Severe design fault/logic vulnerablity related to key business;
- Affect user/company asset, including but not limited to severe payment vulnerablity, digital asset private key leaks, etc;
- Can lead to market manipulation, such as illegal operations that initiate buy/sell trades.
- Can lead to market manipulation, such as unauthorized operations that initiate buy/sell trades

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

- Can directly get backend access privilege;
- Can directly get large amount of sensitive information, including but not limited to source code, SQL input etc;
- Can directly, without interaction, steal large amount of users or backend admin IDs, including but not limited to user visible page storage type XSS, backend visible XSS (Need proof that can access backend information, otherwise would be classified as medium or low risk), etc.

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

- Some amount of sensitive information leaks, including but not limited to SSRF internal network information leaks, partial user information leaks, etc;

- Need interaction, explosion etc to steal user IDs, including but not limited to non-typical page storage type XSS, 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, etc;
- URL jumping vulnerablity;
- Text message interface abuse issues, etc;
- Need complex interaction to steal user IDs, including but not limited to XSS, CSRF, etc;
- Other vulnerbilties where there is no proof of real exploitation, but issues in theory

These vulnerablities are not accepted for the time being(not including Bounty Vendors):

- SPF mail forge vulnerablities
- Vulnerablity steal user account name using Interface exhaust explosion
- Self-xss/Post type XSS vulnerablities that cannot be exploited
- Vulnerabiliy of Denial of Service
- Vulnerabilities of identity theft with high interaction requirements, including but not limited to reflective XSS and general CSRF, etc.
- Vulnerabilities that lead to URL jump
- SMS interface abuse and other problems
- Mail explosion
- Design fault/logic vulnerablity that only affect own account
- Other low impact vulnerablities
- Vulnerablities whose vendor is not in normal operation (abandoned projects, Ponzi scheme projects, etc).

Blockchains/Cryptocurrencies

	Severe	High risk	Medium risk	Low risk
Level 1(ETH)	39.0	27.0	7.5	1.2
Level 2(ETH)	16.9	7.8	3.9	0.7
Level 3(ETH)	6.5	3.6	1.0	0.4
Level 4(ETH)	3.5+1280	1.1+640	0.5+320	0.2+160
Level 5(DVP)	256.0	128.0	64.0	6.0

Level classification data from: https://coinmarketcap.com

Level 1: Market cap top 30

Level 2: Market cap top 100

Level 3: Market cap top 400

Level 4: Market cap below top 400

Level 5: Not in the list, but has daily trading volume

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, passwords, etc.

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

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

- Can lead to local privilege upgrade;
- Design flaws/logic vulnerablities that affect user’ s own account;
- May lead to high risk vulnerablities 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 vulnerablities;
- Can cause system resource abuse or user spam.
- Other vulnerbilties 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

	Severe	High risk	Medium risk	Low risk
Level 1(ETH)	31.2	14.4	4.7	0.6
Level 2(ETH)	5.2	2.3	1.0	0.3
Level 3(ETH)	1.6	0.8	0.4	0.2

Level 4(ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
Level 5(DVP)	256.0	128.0	64.0	6.0

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

Level 1 : the selected wallets in the list below

Ledger	imToken	Metamask	Tronlink
Trust	Trezor	Huobi Wallet	coinbase
Matrixport	Babel	MakerDAO	

Level 2: Total Rank top 30, except the ones in Level 1

Level 3: Total Rank top 80

Level 4: Total Rank below top 80

Level 5: Not in the list, but has some verifiable users

Severe: 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.

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

- 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 bussiness design flaws/logic vulnerablities;
- Non essential bussiness design flaws/logic vulnerablities.

Mining pools

	Severe	High risk	Medium risk	Low risk
Level 1 (ETH)	15	10	5	1
Level 2 (ETH)	6	3	1	0.5
Level 3 (ETH)	2.6	1.5	0.4	0.1

Level Classification data from:https://btc.com/stats/pool

Level 1: Top 10

Level 2: top 20

Level 3：not in top 20 but still in the 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 ming pool reward or wallet money.

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

- 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 vulnerablities that can lead to some risk.

Low risk:

- Can lead to small amount of information leaks
- Can have real impact under specific conditions

DApp

	Severe	High risk	High risk	Low risk
Level 1(ETH)	29.3	18.0	7.5	0.6
Level 2(ETH)	16.9	7.8	3.9	0.3
Level 3(ETH)	6.5	3.6	1.0	0.2
Level 4(ETH+DVP)	3.5+1280	1.1+640	0.5+320	0.1+160
Level 5(DVP)	256.0	128.0	64.0	6.0

Level classification data from:https://dapp.review/explore（7 天交易数）

Level 1: top 10

Level 2: top 50

Level 3: top 200

Level 4: below top 200

Level 5: Not in the list, but has digital asset and daily trading volume

Severe:

- Can unconditionally steal contracts or contract users' digital assets;

High risk:

- 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 vulnerbilties 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

	Severe	High risk	Medium risk	Low risk
Level 1（DVP）	3072	2048	1024	512

Level 2 (DVP)	1024	512	256	128
Level 3 (DVP)	512	256	128	64
Level 4 (DVP)	256	128	64	32
Level 5 (DVP)	64	32	16	8

Severe:

- 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 vulnerablities;

High risk:

- 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 vulnerablities;
- 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: the general website vulnerabilities of one blockchain project.
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 reward standards above

	High risk	Low risk
Level 1(ETH)	0.6	0.2
Level 2(ETH)	0.4	0.1
Level 3 and below(ETH)	256	64

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, 4, 5 classification above

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

- Can obtain system privilage, and there are many sensitive information (more than 120 pieces);
- Can login to sensitive database;
- Can login to sensitive mailbox;
- Can seriously affect users or projects;

Low risk:

- Storage XSS, need to prove background privilage;
- Can login to non-sensitive mailbox;
- Can login 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;
    - 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. And the demotion could have 2 directions.

    - 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**

- Vulnerablity itself doesn’ t have value, their value derives from the harm they can bring, **so the reward of a vulnerablity is decided by vulnerablity 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 vulnerablity 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 vulnerablities not covered by the rewards rules above, DVP may decide to accept them or not.

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

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

- Vulnerablities come from the same source would be counted as one, such as multiple vulnerablities caused by same interface, multiple page vulnerablities caused by same publishing system, whole site vulnerablity 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 vulnerabilies will not be accepted: interface abuse, SMS explosion, 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.

- Some DoS vulnerabilities (including but not limited to conceptual DoS: for example, the server may respond slowly to its users due to the frequent sending of packets to a function point, and may refuse to respond) are not accepted.

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

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

- 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 sealing the account.

- 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.

- 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

- 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 vulnerablities 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 vulnerablity procedure, level classification, reward, etc, please enter comments into vulnerablity detail page or contact online customer service. DVP would coordinate among related parties to resolve conflicts, while giving priority to vulnerablity submitters, and may introduce independent security professionals if necessary.

Reference

Some standards above are referred to Xian Zhi vulnerablity classification standard. Thank you !