Blockchain Security Evolution Global Hackson – Korea Stop

Online Preliminary

Registration time: Now to Oct. 10, 19:00 (UTC+9)

Registration link: https://forms.gle/KU8XvnfWSLpvcs4C9

Preliminary time: Sep. 26, 19:00 (UTC+9) to Oct. 10, 19:00 (UTC+9)

Preliminary Form

search for vulnerabilities of bounties on DVP and other open-source blockchain projects, then submit them on DVP website. More details about the target projects list, reward standards, vulnerability rating rules, and general rules, please check the following parts.

Submit Form: Please submit the vulnerability reports with title "Korea Hackathon + Team name + vulnerability name".

Scoring&Ranking

The score of one team = the rewards of vulnerabilities all team member submitted.

Team ranking is based on the ETH rewards firstly; and if two or more teams have same ETH rewards, team with more DVP will be higher in rank; if two or more teams have both same ETH and DVP rewards, then the team who reach the score first will be higher in rank.

Preliminary Prize

In addition to rewarding the vulnerability submitter according to the reward standard, the top three of all the teams will win special prize as follow.

Total: 50,000 DVP

- No.1 team: 25,000 DVP
- No.2 team: 15,000 DVP
- No.3 team: 10,000 DVP

The top 3 of the international teams, i.e. the non-South Korean teams, will be qualified for the final hackathon in Seoul and have chance to win the 21,000 USD prizes; and the main travel expense of No.1 team will be covered.

Scores and Ranks update:

During the preliminary, scores and ranks of Top 10 Korean teams and Top 3 international teams will be updated and published through Preliminary Leaderboard. Due to the complexity of vulnerabilities, especially verification of vulnerabilities of some public chains, there will be some delay in updating the Preliminary Leaderboard.

The reviewing process is expected to be completed within 48 hours at most after vulnerabilities are submitted.

The final scores and ranks will be published at 19:00 (UTC+9) on Oct 11 through the Preliminary Leaderboard and DVP official Telegram, Kakao, Twitter, Wechat, Weibo

Preliminary Leaderboard: https://dvpnet.io/team

P.S.

- If one team is registered during preliminary time, only the vulnerabilities submitted from that registration time to the end of the preliminary will be scored.
- One team member is not allowed to join different teams at the same time, and also not allowed to change team during preliminary time.
- In a normal process, when vulnerabilities are submitted, DVP will firstly inform the projects and wait them to claim the vulnerabilities within a certain period. After that, the reward will be given to white hat hackers. In order to quickly calculate the scores and ranks during the preliminary, DVP will change the process temporarily. After one vulnerability is admitted and passed by DVP reviewer team, the rewards will be given according to the historical average amount of rewards of this kind of projects and level of severity. When the projects claim the vulnerability, if the rewards are higher than the previous ones, the difference will be given to the white hat hackers; if the rewards are lower than the previous award, the difference shall be borne by DVP foundation. And the

rewards changes will not be updated to the scores, and will not change the final results.

Target list：

- **Bounty Vendors**

  Exchange: Bibox, Gate.io, Chaince, 60.COM, Coinw, HashExchange, DigiFinex, mxc, BKEX, wankejia, FUBT, bitrabbit, NEEX, pk.top

  Public chain/Token: Elastos, Vechain, Contentos, BOSCORE, Showcoin, G.game, Contentos, Lambda, NEST Protocol, NEO, YEE, Aurora(AOA), Force protocol, Bytom, everiToken, GXChain, Achain, DAD, Nest protocol, Linkchain, YEE, G.game.

  Mining pool: F2Pool, Liebi

  Wallet: Kcash, Mathwallet, HOO.

  Others: PechShield, BCSEC, DVP, feixiaohao,

- **Open source projects**

  Public Chain/Token：https://coinmarketcap.com/coins

  DAPP：https://www.dapp.com/

Reward Standards :

Exchange	Name	Reward	Severe	High risk	Medium risk	Low risk
	Bibox	ETH	14	4.5	1.6	0.125
	Gate.io	ETH	14	4.5	1.6	0.125
	MXC	ETH	10	3.5	1.25	0.275
	BKEX	ETH	3.5	0.85	0.45	0.125
	Coinw	ETH	12.5	3.5	0.6	0.125
	DigiFinex	ETH	12	4.5	1.6	0.125
	FUBT	ETH	1.5	0.75	0.35	0.125
	60.COM	ETH	13	4	1.1	0.125
	Bitrabbit	ETH	0.75	0.3	0.09	0.065
	Chaince	ETH	14	4.5	1.6	0.125
	HashExchange	ETH	12.5	3	0.65	0.175
	pk.top	ETH	0.75	0.35	0.15	0.075
	wankejia	ETH	1.5	0.75	0.35	0.125
	NEEX	ETH	0.75	0.35	0.15	0.075

Public Chain/Token (Open-source projects)	https://coinmarketcap.com/coins/				
Level	**Reward**	**Severe**	**High risk**	**Medium risk**	**Low risk**
Level 1: top 30	ETH	39	27	7.5	1.2
Level 2: top 30-100	ETH	16.9	7.8	3.9	0.7
Level 3: top 30-500	ETH	6.5	3.6	1	0.4
Level 4: below top 500	ETH+DVP	3.5+1280	1.1+640	0.5+320	0.2+160
Level 5: Not in the list, but traded daily and has ICO	DVP	256	128	64	6

Public Chain/Token (DVP bounty)	Name	Reward	Severe	High risk	Medium risk	Low risk
	Elastos	ETH	25	12.5	3	0.525
	LinkChain	ETH	19	6	2.2	0.225
	VeChain	ETH	49.5	24.5	12	4.025

	Lambda	ETH	7	3.5	1.6	0.125
	Bytom	ETH	6.225	2.9	1.025	0.225
	GXChain	ETH	6	3	1.1	0.125
	Aurora(AOA)	ETH	1.15	0.55	0.2	0.075
	Achain	ETH	1.15	0.55	0.2	0.075
	Contentos	ETH	8	4.5	1.6	0.125
	BOSCORE	ETH	20	7.5	3	0.525
	Showcoin	ETH	14.5	3.225	1.275	0.075
	YEE	ETH	3	1.5	0.55	0.075
	The Force protocol	ETH	0.9	0.65	0.4	0.175
	everiToken	ETH	14	4.5	1.6	0.125
	DAD	ETH	0.9	0.65	0.4	0.175
	G.game	ETH	11.5	6.5	3	0.525

Thanks the special support from Elastos community, Elastos welcome all white hat hackers to help build the ecosystem.

Mining pool	**Name**	**Reward**	**Severe**	**High risk**	**Medium risk**	**Low risk**
	Liebi	ETH	4	2	0.55	0.075
	F2Pool	ETH	0.9	0.65	0.4	0.175

Wallet	**Name**	**Reward**	**Severe**	**High risk**	**Medium risk**	**Low risk**
	Kcash	ETH	12.5	3	0.6	0.125
	Mathwallet	ETH	1.5	0.75	0.35	0.125
	HOO	ETH	0.09	0.075	0.065	0.055

DAPP (Open-source projects)	https://www.dapp.com/				
Level	**Reward**	**Severe**	**High risk**	**Medium risk**	**Low risk**
Level 1: top 10	ETH	29.3	18	7.5	0.6
Level 2: top 10-50	ETH	16.9	7.8	3.9	0.3
Level 3: top 50-200	ETH	6.5	3.6	1	0.2
Level 4: below top 200	ETH+DVP	3.5+1280	1.1+640	0.5+320	0.1+160

Level 5: Not in the list but has digital asset and daily trade	DVP	256	128	64	6

Others	Name	Reward	Severe	High risk	Medium risk	Low risk
	PeckShield	ETH	11	1.5	0.6	0.125
	BCSEC	ETH	11	1.5	0.6	0.125
	DVP	ETH	9.5	2.5	1.5	0.525
	feixiaohao	ETH	1.69	0.94	0.265	0.07

Vulnerability rating rules

Public Chain

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

• Can remotely get access privilege;

• Can directly steal digital assets;

• Severe sensitive information exposure, including but not limited to user private keys, passwords, etc.

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

• Can lead to denial of services;

• Design faults/logic loopholes that affect large amount of users/exchanges

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

• Can lead to local privilege upgrade;

• Design faults/logic loopholes that affect user’ s own account;

• May lead to high risk loopholes indirectly.

Low risk:

• General information exposure;

• Low effect design faults/logic loopholes;

• Loops that can cause system resource abuse or user spam.

Wallets

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

• Can unconditionally remote get service/client access privileges;

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

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

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

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

• 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 in theory only

• Can lead to malicious changes of user information;

• Can lead to malicious changes of user information;

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

Low risk:

• General information exposure;

• Non-essential business design faults/logic loopholes;

• Non-essential business design faults/logic loopholes.

DAPP

Severe:

• Can unconditionally steal contracts or contract users’ digital assets.

Can unconditionally steal contracts or contract users’ digital assets

• Can unconditionally steal contracts or contract users’ digital assets;

• Can unconditionally use contracts' important functions or denial of services.

Medium risk:

• Can create or destroy some users' digital assets;

• Can steal limited contracts or contract users' digital assets.

Low risk:

• Security loopholes in theory, including but not limited to loopholes only can be exploited by owners.

Mining Pool

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

• Can unconditionally remote get mining pool all privileges;

• Can unconditionally remote control all mining pool computation power;

• Can unconditionally steal mining pool reward or wallet money.

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

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

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

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

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

• Design faults/logic loopholes that can lead to some effect.

Low risk:

• Can lead to small amount information exposure

• Loopholes can have real effect under some conditions

Exchange

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

• Can directly get system privilege;

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

• Affect user/company asset, including but not limited to severe payment loophole, digital asset private key exposure, etc.;

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

• 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, SQL input etc.;

• Loopholes that can directly, without interaction, steal large amount of users or backend employees' 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.

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

• Small amount of sensitive information exposure, including but not limited to SSRF internal network information exposure, partial user information exposure, etc.;

• Design fault/Logic loophole that only affect user’ s own account;

• Loopholes that need interaction, explosion etc. to steal user IDs, including but not limited to non-typical page storage type XSS, backend invisible XSS;

• Denial of service loophole;

Low risk: No proof of real exploitation, issues in theory only

• Non-Sensitive information exposure, including but not limited to directory traverse, etc.;

• URL jumping loophole;

• Short message interface abuse issues, etc.;

• Loopholes that highly interactive, steal user IDs, including but not limited to XSS, CSRF, etc;

• Loopholes that highly interactive, steal user IDs, including but not limited to XSS, CSRF, etc.

These loopholes are not admitted for the time being:

• SPF mail forge loopholes

• Loophole steal user account name using Interface exhaust explosion

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

• Mail explosion

• Not sensitive operation CSRF issues

• Other low effect loopholes

• Loopholes of non-operative sites or Ponzi scheme sites

General rules

Loopholes per se don’ t have value, their value derives from the harm they can bring, so the reward of a loophole discovery is decided by loophole information submitted by white hats, and its effect range and difficulty of its exploitation, If the triggering condition is very strict, including but not limited to, XSS loophole in some specific browsers, the reward level can be adjusted.: the auditors don’ t speculate on the harm of a loophole can bring, all proof has to be in the loophole information submission, not effect only in theory!

For loopholes not covered by any classification rules, DVP may decide to or not to record them.

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

The reward objects (public chains, exchanges, etc.) in the reward criteria are limited to themselves. If they submit loopholes in other assets (official websites, APPs, etc.) of their manufacturers, they will be downgraded according to the actual business situation.

For general loophole submissions, please list vendors’ information or how to search them, and submit at least five operating sites as case examples.

Loopholes come from the same source would be counted as one, such as multiple loopholes caused by same interface, multiple page security loopholes caused by same

publishing system, framework causing whole site security loophole, security issues caused by DNS, or same file with different parameters, etc.

Third party product loopholes, including but not limited to, Wordpress used by companies, flash, or Apache components, OpenSSL, SDK, etc. Same loophole with different software versions is regarded as one.

Same loophole, but later submission has different way of exploitation, all submissions will pass, but part of the reward for later submissions will be given to the first submission.

Submitters cannot publish or submit loophole details to other platforms, otherwise their account and asset may be frozen.

If loophole exploitation need privileged account, or can only be triggered under certain conditions, the reward may be lowered.

Loophole grouping

For related loopholes, such as using weak password to get into backend system, or SQL input, auditors may increase the loophole level. Later discoveries can be added into the same loophole, and the reward may be increased.

For one loophole submitted as multiple, DVP may group them together as one, it would be classified using highest level, but rewarded by applying the lowest standard. If they are done on purpose, submitters account may be disabled.

Submitter’ s account and asset may be frozen in the following cases:

For ordered loopholes, submit the later ones first. Such as, discovery of weak mailbox password, then use the password to get backend administrator password, submitting the backend password first, then mailbox weak password second.

Using testing loophole as excuse, using loophole to harm users' interest, affect users' business, DVP would not issue reward, but may disable its account and assets.

For vendors DVP decided not to record, loophole submissions would be returned temporarily. After vendors follow DVP recording standard, loopholes can be resubmitted, and reward will be issued according to submission time.

For submissions without clear explanation, they would be rejected immediately. Every loophole submission needs to include loophole's URL, text details, complete graph, and clear explanation, such as:

Vendor and it's website, if there is no IP address of the website, then need separate explanation.

Loophole details need to have all related URLs

Loophole proofs need to list all key steps, meaning auditors can reproduce it using these steps

Loophole related payload, need to be included in the loophole detail text, or as screenshot

For marginal or abandoned systems, the reward level would be lowered

Information exposure type loopholes, such as GitHub information exposure, memcache, redis unauthorized access, etc, level classification would be according to contents validity and sensitivity, and isolate and low risk exposures may be ignored

Backend explosion issues need to be have proof of successful exploitation, otherwise they would be rejected.

Weak password issues:

Different weak passwords in the same system discovered by same submitter would be regarded as one case.

Default initial password is regarded as on case.

For non-essential systems, only the first weak password submission will accepted.

For essential systems and key business, the first two-week password submissions will be accepted.

For related loopholes, don’ t submit as multiple cases, otherwise DVP may freeze submitters assets.

Don’ t execute tests which may cause service disruptions, such as IIS denial service or slow_http_dos etc.

If a service has both the PC site and mobile app site, and they use same interface and source code, same loophole from PC and app sites would be regarded as the same one.

About information exposure loopholes, submissions with real exploitation examples would be regarded as severe or high risk; key service config or source code exposure would be regarded as medium risk, no exploitation example or not key business related, would be regarded as low risk or rejected.

The rules of this event are subject to further interpretations and/or modifications made by DVP.