社区规则 v5.0

更新日期：2020.04.03

漏洞收集协议

为使 DVP 社区漏洞收集流程化、规范化、标准化，社区成员 BCSEC 和 PeckShield 撰写了该协议用以打造早期的社区共识，该协议会根据社区反馈进行逐步更新迭代。

收集范围

A 类 :已入驻厂商（漏洞赏金厂商），漏洞直接由厂商认领或者不认领。

B 类: 非入驻厂商（非漏洞赏金厂商），旗下有与区块链相关产品的厂商，类型包含但不限于与区块链相关的交易所、加密货币、软硬件等等。在收到此类厂商的有效漏洞报告后，DVP 会先联系厂商来认领，若始终无人响应，则暂时由 DVP 社区代为认领。 注意： **B 类厂商不是固定的，随时会视实际情况降为 C 类厂商**

C 类 :非收录厂商， **该类厂商是 DVP 基金会明确决定已经不再收取的** ，包括但不限于资讯类站点（行情快讯等）、电商类站点（售卖矿机等）等与区块链、加密货币没有直接关联或非正常运营（废弃项目、诈骗项目等）的厂商。

B 类厂商相关说明

以下奖励标准仅针对 B 类厂商， 漏洞的奖励金额最终取决于漏洞的**实际影响。**当实际影响低于漏洞本身的危害时，**降级规则**将在此适用。

- 所有漏洞或威胁情报都需要满足未公开、未修复、未在其他平台提交这三个条件。
- 若目标类型不在奖励范围（代币、交易所、公链.....）内，但该目标在区块链产业中具有一定的影响力，可以先以威胁情报提交，奖励根据漏洞实际危害进行评定。
- 审核员不会对漏洞危害进行任何推测，一切都需要在漏洞详情中实际证明出来，DVP 不接受仅理论上成立的漏洞。
- 若漏洞类型属于相应厂商的非主营业务，对应奖励请参见非核心漏洞栏目。
- 对于确实有一定危害但没在奖励规则中提到的漏洞或者奖励规则不合理等问题，后续会根据社区的反馈进行更新，此为 4.0 版本，之后会持续根据社区反馈进行版本迭代。
- 漏洞奖励根据漏洞实际情况进行取值，表格中的奖励为最高奖励额度，单位是 ETH。
- DVP 对厂商等级和漏洞等级进行了定义，请在提交漏洞报告时正确选择并附上链接，审核人员会进行验证，若故意选择错误等级，将会被记录并惩罚。
- 若漏洞/威胁情报无法根据该版本的协议进行定义，则根据 CVSS 漏洞评级标准和实际影响情况进行判定。

- 在提交漏洞时，请在漏洞详情中附上提交时刻的厂商排名截图，并将日期时间也截取在内并标注。DVP 审核时，会先确认截图真实性，截图真实则优先使用截图中的排名；若故意使用错误截图误导审核，DVP 将进行严厉处罚；若无截图，则默认使用审核时所见排名。

奖励标准

交易所

	严重	高危	中危	低危
一等(ETH)	31.2	14.4	4.7	0.6
二等(ETH)	5.2	2.3	1.0	0.3
三等(ETH)	1.6	0.8	0.4	0.2
四等(ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
五等(DVP)	256	128	64	6

评判依据：https://www.feixiaohao.com/exchange/

一等交易所名单：

币安	火币	Coinbase Pro	OKEX
Bithumb	Gate.io	Bittrex	Poloniex
Bitstamp	Bitflyer	Gemini	Upbit
BitMEX	Bitfinex	Kraken	Bakkt
ZB			

二等：非小号综合排名前 50 中，除社区一等交易所名单以外的厂商。（部分优质二等厂商可能会在奖励标准之上追加额外奖励，则 DVP 会将该额外奖励发放给相应白帽子）

三等：综合排名前 80

四等：综合排名前 120

五等：没有在非小号交易平台综合排行前 120 名，但是至少一个币种每日有交易量

严重：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可直接获得系统权限；

• 涉及到核心业务的严重设计缺陷/逻辑漏洞；

• 影响用户/企业资产，包括但不限于严重的支付漏洞、数字资产私钥泄露等；

• 可导致市场操纵，例如越权操作大量用户下发买单、埋单等；

高危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可直接获得后台权限；

• 可直接获取大量敏感信息，包括但不限于源代码泄露、SQL 注入等；

• 可无需交互直接盗用大量用户或后台人员身份凭证的漏洞，包括但不限于大量用户可见页面存储型的 XSS、后台可见的 XSS（需要实际证明获取到了后台信息，否则按中低危评判）等；

中危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 部分敏感信息泄露，包括但不限于 SSRF 内网信息泄露、用户部分信息泄露等；

• 需要交互、爆破等手段盗用其他用户身份凭证的漏洞，包括但不限于非常用页面存储型 XSS、后台不可见 XSS；

低危：没有真实利用成功证明但理论存在的隐患都可归为此类

• 非敏感信息泄露，包括但不限于目录遍历等；

• 其他未证明实际危害但理论存在的隐患；

暂不收取（不包括入驻厂商）：

- SPF 邮件伪造漏洞
- 接口穷举爆破已注册用户名类漏洞
- 无法利用的 Self-XSS / POST 方法反射型 XSS
- 交互要求较高的盗用身份凭证的漏洞，包括但不限于反射型 XSS、普通 CSRF 等；
- URL 跳转漏洞；
- 短信接口滥用等问题；
- 拒绝服务漏洞；
- 邮件轰炸
- 已无人运营的废弃站点或诈骗、传销项目站点
- 仅影响自己账户的设计缺陷/逻辑漏洞
- 其它危害过低的漏洞

区块链/加密货币

	严重	高危	中危	低危
一等(ETH)	39.0	27.0	7.5	1.2
二等(ETH)	16.9	7.8	3.9	0.7
三等(ETH)	6.5	3.6	1.0	0.4
四等(ETH+DVP)	3.5+1280	1.1+640	0.5+320	0.2+160
五等(DVP)	256.0	128.0	64.0	6.0

评判依据：https://coinmarketcap.com

一等：市值排名前 30

二等：市值排名前 100

三等：市值排名前 400

四等：市值排名前 400 之外

五等：没在排行榜中但是具有一定规模且每日都有交易

严重：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可直接远程获取权限；

• 可直接导致数字资产被窃取；

• 严重的敏感信息泄露，包括但不限于用户私钥、密码等；

高危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可直接导致拒绝服务；

• 影响大量用户/交易所的设计缺陷/逻辑漏洞；

• 可无条件造成数字资产任意量增发或销毁；

• 可无条件使合约重要功能拒绝服务；

中危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可导致本地权限提升；

• 仅影响自己账户的设计缺陷/逻辑漏洞；

• 可间接产生高危影响的漏洞；

• 可使有限的用户数字资产额外增发或销毁；

• 可有限地窃取合约内或合约用户的数字资产；

低危：

• 普通信息泄露；

• 实际危害较低的设计缺陷/逻辑漏洞；

• 可导致系统资源滥用或用户骚扰的漏洞；

• 仅理论上存在危害的安全隐患包含但不限于 owner 才能利用的漏洞等；

钱包

	严重	高危	中危	低危
一等(ETH)	31.2	14.4	4.7	0.6
二等(ETH)	5.2	2.3	1.0	0.3
三等(ETH)	1.6	0.8	0.4	0.2
四等(ETH+DVP)	1.2+640	0.6+320	0.3+160	0.1+80
五等(DVP)	256.0	128.0	64.0	6.0

评判依据：https://www.feixiaohao.com/wallet/

一等钱包名单：

Ledger	imToken	Metamask	Tronlink
Trust	Trezor	火币钱包	coinbase
Matrixport	Babel	MakerDAO	

二等：非小号综合排名前 30 中，除社区一等钱包名单以外的厂商

三等：排名前 80

四等：排名前 80 之外

五等：没在排行榜中但是可以证明其有一定用户量

严重：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可无条件导致服务端/客户端权限被远程获取；

• 可无条件导致大量数字资产被窃取；

• 可无条件导致严重的敏感信息泄露，包括但不限于用户私钥、密码等；

高危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可无条件导致大量敏感信息泄露；

• 可无条件导致服务端/客户端拒绝访问

• 可无条件导致大量用户身份被盗用

中危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可导致用户信息被恶意篡改

• 可导致部分敏感信息泄露

• 可无条件导致少量用户身份被盗用

低危：

普通信息泄露；

• 实际危害较低的设计缺陷/逻辑漏洞；

• 可导致系统资源滥用或用户骚扰的漏洞；

矿池

	严重	高危	中危	低危
一等（ETH）	15	10	5	1
二等（ETH）	6	3	1	0.5
三等（ETH）	2.6	1.5	0.4	0.1

参考依据：https://btc.com/stats/pool?pool_mode=year

一等：排名前 10

二等：排名前 20

三等：排名前 20 以外，且仍在排行榜中

严重：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可无条件直接远程获取矿池所有权限；

• 可无条件直接远程控制矿池所有算力；

• 可无条件窃取矿池挖矿奖励或矿池钱包资金；

高危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可无条件导致矿池核心业务拒绝服务；

• 可无条件导致矿池利益收到损害，例如扣块攻击、伪造算力等；

• 可无条件导致大量敏感信息泄露；

中危：需要有真实利用成功的证明，不认可仅理论存在的问题。

• 可以导致产生一定危害的设计缺陷/逻辑漏洞；

低危：

• 可导致少量的信息泄露

• 具有一定条件才能造成实际危害的漏洞

DApp

	严重	高危	中危	低危
一等(ETH)	29.3	18.0	7.5	0.6
二等(ETH)	16.9	7.8	3.9	0.3

三等(ETH)	6.5	3.6	1.0	0.2
四等(ETH+DVP)	3.5+1280	1.1+640	0.5+320	0.1+160
五等(DVP)	256.0	128.0	64.0	6.0

判断依据：https://dapp.review/explore（7 天交易数）

一等：排名前 10

二等：市值排名前 50

三等：市值排名前 200

四等：市值排名前 200 之外

五等：没在排行榜中但是 DApp 中有一定额度数字资产且每日都有交易

严重：

• 可无条件任意窃取合约内或合约用户的的数字资产；

高危：

• 可无条件造成数字资产任意量增发或销毁；

• 可无条件使合约重要功能拒绝服务；

中危：

• 可使有限的用户数字资产额外增发或销毁；

• 可有限地窃取合约内或合约用户的数字资产；

低危：

• 仅理论上存在危害的安全隐患包含但不限于 owner 才能利用的漏洞等；

威胁情报

	严重	高危	中危	低危
一等（DVP）	3072	2048	1024	512
二等（DVP）	1024	512	256	128
三等（DVP）	512	256	128	64
四等（DVP）	256	128	64	32
五等（DVP）	64	32	16	8

严重：

• 区块链相关大量敏感信息泄露相关确凿证据；

• 非个人的大量数字资产窃取相关确凿证据；

• 区块链相关未公开严重漏洞利用确凿证据；

高危：

• 区块链产业相关知名厂商被入侵相关确凿证据；

• 针对区块链相关产业进行大型攻击的确凿证据；

• 区块链相关软硬件存在后门的确凿证据；

• 针对区块链相关产业的新型攻击方式；

中危：

• 区块链相关漏洞被利用相关线索；

• 区块链热点安全事件未公开线索；

• 针对区块链厂商的敏感信息泄露；

低危：

• 区块链相关仿冒网站、App 等；

• 针对区块链相关产业攻击的相关线索；

非核心漏洞

此处“非核心漏洞”泛指区块链项目的非主营业务相关漏洞。

举例：区块链/数字代币、钱包、Dapp 的网页相关漏洞等

若“非核心漏洞”可以对主营业务造成危害，也符合一般规则的判定条件，则按照一般规则处理

	高危	低危
一等（ETH）	0.6	0.2
二等（ETH）	0.4	0.1
三等或以下（DVP）	256	64

一等：项目所属分类的一等厂商；

二等：项目所属分类的二等厂商；

三等或以下：项目所属分类的三等或更低等级厂商；

高危：

• 需要有真实利用成功的证明，不认可仅理论存在的问题；

• 可得系统权限，且其中敏感信息较多（大于 120 条）；

• 敏感数据库登录；

• 敏感邮箱登录；

• 影响用户或企业的相关严重问题；

低危：

• 需要有真实利用成功的证明，不认可仅理论存在的问题；

• 存储型 XSS，需要证明后台权限；

- 非敏感邮箱登录；
- 非主要数据库登录；
- 少量敏感信息泄露；

降级规则

- 漏洞奖励的最终标准，取决于漏洞的实际影响。
- 漏洞的实际影响由多个维度决定，包括但不限于漏洞本身的危害，漏洞的利用难度、影响范围，和黑客利用后可实际导致的影响后果等。
- 当漏洞的实际影响低于漏洞本身的危害时，DVP 基金会将根据以下规则对漏洞进行降级处理。
- 降级的判定条件：
  - 测试环境下的测试数据；
  - 对于边缘/废弃业务系统；
  - 漏洞利用过程中需要涉及非普通用户权限，或在满足一定条件下才能触发；
  - 同一系统多个弱口令；
  - 其他 DVP 基金会认定的降级情况。
- 漏洞降级最多不超过一级
  - 举例：2 等厂商的中危漏洞会被降为 2 等厂商的低危漏洞。
  - 举例：2 等厂商的低危漏洞会被降为 3 等厂商的低危漏洞。

通用原则

- 除了入驻厂商，适用其他厂商类别
- 漏洞本身没有价值，其能造成的最大危害才是其真正的价值，所以漏洞的 最终奖励额度由白帽子提交的漏洞详情所直接体现出来的利用难度及影响范围等综合因素决定 ，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的 XSS 漏洞，则可跨等级调整奖励。注意： 审核员不会对漏洞危害进行任何推测，一切都需要在漏洞详情中实际证明出来，不接受仅理论上成立！
- 对于没有在任何一项评判依据内的厂商的漏洞，DVP 基金会会酌情选择收录，但同时 DVP 基金会也有权选择暂不收录。
- 若同一漏洞在不同厂商之间出现不下 3 次则将被认定为通用漏洞，3 次之后其他厂商若被提交此漏洞则评为重复漏洞，但漏洞依然保留，用作厂商认领。
- 奖励标准中的悬赏对象（公链、交易所等）仅限于其本身，若提交其厂商旗下的其他的资产（官网、APP 等）的漏洞，则根据实际业务情况进行等级降级。
- 若提交通用漏洞，必须要写明厂商信息或着给出 准确的 检索语法，同时还需要提交至少 5 个非废弃站点作为案例。
- 对于通用漏洞奖励，将根据受影响的厂商中排名靠前的厂商进行计算：受影响的厂商中，排名前三的厂商按照规则给与奖励，然后再给予一份奖励

为前三厂商奖励的平均值，即，3 个排名靠前厂商的奖励+（3 个排名靠前厂商的奖励/3）。

- 同一个漏洞源产生的多个漏洞计漏洞数量为一。例如同一个接口引起的多个安全漏洞、同一个发布系统引起的多个页面的安全漏洞、框架导致的整站的安全漏洞、泛域名解析产生的多个安全漏洞；因为厂商未做身份校验导致的同一系统多个接口越权或者是未做 token 校验导致的多个 CSRF 漏洞；同一文件的不同参数、同一参数出现在不同文件、同一文件在不同目录等。
- 接口滥用/短信轰炸，API 文档泄露，URL 跳转，反射型 XSS，DOM-Based XSS，交互要求较高的 CSRF/JSONP Hijacking/CORS 劫持敏感信息，等一系列低风险、低危害、高交互的问题暂不纳入漏洞接收范围。
- 对于上传到 OSS/Bucket 等等的存储型 XSS，将会根据漏洞真实危害情况酌情降低漏洞等级/赏金或者拒绝处理
- 部分拒绝服务漏洞（包括但不仅限于概念性拒绝服务: 例如频繁向某处功能点发包导致服务端对自身用户的响应缓慢，拒绝响应等问题）概不纳入漏洞接收范围。
- 具有较高利用难度的用户部分信息泄露或设计缺陷，将不纳入漏洞接收范围。
- 第三方产品的漏洞包括但不限于企业所使用的 WordPress、Flash 插件以及 Apache 等服务端相关组件、OpenSSL、第三方 SDK 等；不同版本的同一处漏洞视为相同漏洞。

- 同一漏洞，后提交的利用方式比第一个提交的利用造成的影响差距过大时，两个漏洞都通过，从第二个漏洞中分一部分奖金给第一个提交的白帽子。
- 不可公开或向其他平台提交已提交的漏洞细节，违者将由 DVP 仲裁组织进行冻结资产并封号处理。
- 漏洞利用过程中需要涉及非普通用户权限，或在满足一定条件下才能触发的漏洞，将会酌情降级或降低奖励。
- 漏洞打包问题
  - 存在前后关系的漏洞，比如同一人提交的弱口令进入后台，后台 SQL 注入或者越权的漏洞合并处理，审核可以酌情提高漏洞等级。若已提交，后面又发现，则补充到该漏洞下面，可以提高奖金金额。
  - 对于漏洞拆分提交者，由 DVP 审核对漏洞进行打包，漏洞等级按打包漏洞中危害最高的计算，奖金按标准的最低额度发放。对于严重拆分漏洞，刷漏洞等恶意行为进行冻结账户、甚至封号处理。
- 若存在以下情况者，将可能会 DVP 仲裁组织进行冻结资产处理。
  - 存在前后关系，先提交后者的。例如：发现邮箱弱口令，从邮箱中获知后台管理员密码，提交漏洞时先提交后台弱口令，再提交邮箱弱口令者。
- 以测试漏洞为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，将不给予奖励，同时由 DVP 仲裁组织进行冻结资产并封号处理。

- 对于非收录厂商的漏洞，DVP 基金会会暂时驳回处理，待厂商符合要求之后，会重新开始收录该厂商的漏洞，如出现重复漏洞，收录原则以开始收录后提交先后顺序为准，之前驳回的漏洞可以重新提交。
- 对于提交描述不清的漏洞，将会直接驳回处理；每个漏洞需要明确产生漏洞的 URL 地址、文字细节、完整的截图、清晰的语言表达，例如：
  - 厂商必须与域名对应，若有对应的域名不能以 ip 提交，若没有域名需要额外说明。
  - 漏洞详情中必须在顶部贴出所有与漏洞相关 URL
  - 漏洞证明中对漏洞的验证步骤必须细致到每一处关键操作，换言之就是审核员可以完全按照漏洞证明中的步骤完整复现漏洞
  - 对于漏洞中使用的相关 payload，必须以文字形式贴入漏洞详情中，不可仅以截图的方式展现
- 对于边缘/废弃业务系统，根据实际情况酌情降级
- 信息泄露类的漏洞如 github 信息泄露，memcache、redis 等未授权访问等，根据存储的内容的有效、敏感程度进行确认评级，单独的危害较低的信息泄露如路径泄露等将会忽略处理。
- 前台撞库、爆破类漏洞，需有成功案例证明；后台爆破，仅收取成功登陆的案例，仅能爆破但没有进入后台的漏洞将驳回。
- 弱口令问题（正常对外可注册的系统不算在弱口令范围内）：
  - 对于同一个人发现同一系统的不同的弱口令，将合并处理（如果厂商已经处理了之前的弱口令，后面再次提交的降级处理，第二次以后提交的都会合并处理）。

- 对于默认的初始密码，只按照一个漏洞进行处理(比如邮箱的初始密码都是同一个密码，视为一个漏洞)。
- 对于非重点系统，审核过程只正常确认该系统的第一个弱口令，后续提交的弱口令酌情忽略处理。
- 对于重点系统或者核心业务，在评级过程中只正常确认前 2 个弱口令，后续的提交弱口令问题酌情降级或者忽略处理。

- 存在前后关系的漏洞，比如同一人提交的弱口令进入后台，后台 SQL 注入的漏洞合并处理，可以提高漏洞等级，希望大家不要拆分漏洞，DVP 平台将根据实际情况对严重拆分漏洞，刷漏洞等恶意行为由 DVP 仲裁组织进行冻结资产处理。
- 切勿进行可能引起业务异常运行的测试，例如：IIS 的拒绝服务或者 slow_http_dos 等漏洞。
- 对于 PC 端和 APP 端同一接口同一套代码的两个漏洞（即使域名可能不同），同一白帽子分开提交平台将会合并处理，主动合并会酌情提高奖励；不同的白帽子分别提交，在厂商未修复之前，算为重复漏洞。
- 对于信息泄露相关漏洞（包括 GITHUB，提交的时候请说明，有哪些特征可以证明是某厂商的），可以深入利用造成很大危害的，高危或者严重；对于是厂商线上对外核心应用服务配置、代码等信息泄露，一般为中危；如果不能做出有效利用且非核心业务的的，低危或者驳回处理。

厂商保护

如果同一个系统中发现了大量（3 个以上）的同类型高危漏洞（如 SQL 注入、命令执行等），审核人员判定该系统几乎没有做任何防护，在收取前 3 个该类漏洞之后其他同类型漏洞均降级处理。

争议解决

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过漏洞详情页面的留言板或者通过即时通讯联系在线工作人员及时沟通。DVP 平台将按照漏洞报告者利益优先的原则与企业三方协调处理，必要时可引入外部安全人士共同裁定。

参考

该版本部分内容参考了先知众测漏洞定级标准，在此表示感谢。