버그 바운티 규칙 v6.0

업데이트 시간: 2021.05.17

버그 바운티 협약

DVP 플랫폼의 취약점 심사 기준을 보다 표준화하기 위해 BCSEC 와 PeckShield 가 버그 바운티 규칙을 작성하였으며 이 규칙은 DVP 커뮤니티의 의견에 따라 조율 및 수정될 수 있습니다.

포상 범위

A 타입: DVP 플랫폼에 가입되어 있는 바운티 기업이며 이 경우 기업에서 직접 수령하거나 거절합니다.

B 타입: DVP 플랫폼에 가입되어 있지 않은 기업이며 이 경우 포상 범위는 블록체인 관련 거래소, 가상화폐 토큰, 디앱, 지갑, 마이닝풀 등이 포함되며 해당 기업이 DVP 플랫폼에 가입하기전까지 DVP 재단에서 대신 수령합니다. 이러한 기업과 관련된 취약점을 제보받은 후 DVP 는 먼저 기업에 확인합니다. 만약 관련 답변이 없을 경우 DVP 에서 일시적으로 1등급 업체의 취약점을 대신 수령하게 됩니다. 기타는 동일하게 4 등급 기업의 포상금 기준에 따라 화이트해커에게 포상금을 지급하게 됩니다.

참고: B 타입 기업의 경우 고정적이지 않으며 실제 상황에 따라 C 타입 기업으로 변경될 수 있습니다.

C 타입: DVP 에서 수령하지 않는 기업이며 이 경우 DVP 재단의 포상범위에 속하지 않음을 명확히 규정합니다. 블록체인 관련 미디어 사이트(뉴스/기사 등), 전자상거래 사이트(채굴기 판매 등) 블록체인/가상화폐와 직접적인 관련이 없거나 정상적으로 운영이 되고 있지 않는 기업 (스캠/사기 등) 등등이 이러한 경우에 포함됩니다.

A 타입 기업 상세 설명:

• 입주기업과 재차 연락이 되지않을 경우, 혹은 취약점에 대해 효과적으로 대응하지 않으면, 커뮤니티는 입주기업이 사전에 지급한 포상금을 사용하여 화이트해커에게 지급 할 것이며, 만약 금액이 부족할 시 커뮤니티는 해당 입주기업의 취약점 수록을 일시 중단할 것입니다.

• 취약점의 영향 및 등급 책정에 이의가 없으나 포상금에 의문이 있고 여러 차례의 조율이 이루어지지 않을 경우, 커뮤니티는 입주기업의 포상금 계획에 따라 해당 기업이 예치한 포상금을 사용하게 되며, 만약 금액이 부족할 경우 커뮤니티는 적절한 보조금을 지급하고 해당 입주기업을 해제할 것입니다.

B 타입 기업 상세 설명:

아래의 포상금 기준은 B 타입 기업에만 적용됩니다. 포상금은 해당 취약점이 실질적으로 미칠 수 있는 영향을 근거로 책정됩니다. 만약 실질적 영향이 매우 낮은 경우 DVP 의 강등 규칙에 따라 포상금이 낮아질 수 있습니다.

- 모든 유효 취약점과 위협 정보(threat information)는 아래의 3 가지 조건을 충족해야 합니다. 1. 공개되지 않은 취약점 2. 패치되지 않은 취약점 3. 타 플랫폼에 제출되지 않은 취약점
- 제출한 취약점 타깃이 포상범위(토큰/퍼블릭체인/거래소/지갑/디앱/마이닝풀 등)에 속하지 않지만 블록체인 업계에서 충분한 영향력이 있을 경우 위협 정보로 제출하실 수 있으며 포상금은 실제 위협 정도에 따라 책정됩니다.

- 심사위원은 제보된 취약점에 대하여 추측을 하지 않습니다. 취약점에 대한 상세한 설명으로 증명해야 하며 DVP 는 이론상으로만 존재하는 취약점은 승인하지 않습니다.
- 제출한 취약점이 타깃 기업의 주요 업무에 속하지 않을 경우 비핵심업무 취약점 기준을 참고하여 주세요.
- 본 버그 바운티 규칙은 4.0 버전으로 확실한 위협이 있지만 규칙에 명시되어 있지 않는 취약점 또는 포상금 기준이 불합리한 문제가 발생할 경우 커뮤니티의 의견에 따라 지속적으로 업그레이드 할 예정입니다.
- 취약점 포상금은 실제 심사 결과에 따라 책정되며 도표에 표시되어 있는 ETH 와 DVP 포상액은 해당 등급의 최고 금액 입니다.
- DVP 에서는 타깃 기업에 대해서도 등급 제도를 실시하며 취약점 제보시 해당 타깃의 등급을 확인할 수 있는 링크를 첨부해주셔야 합니다.
- 취약점/위협 정보가 DVP 버그 바운티 규칙으로 책정이 불가할 경우에는 CVSS 취약점 등급 기준과 실제 위협 정도에 따라서 판단됩니다.
- 취약점 보고서 제출 시 제출 시점에 타깃 기업의 랭킹을 확인할 수 있는 스크린샷을 첨부하여 주십시오. DVP 에서는 첨부된 스크린샷의 정확성을 확인한 후 해당 시점의 랭킹을 기준으로 심사를 진행할 것이며 고의적으로 잘못된 정보를 제출하는 행위가 발견될 경우에는 패널티가 있을 예정입니다. 스크린샷이 첨부되지 않았을 경우에는 DVP 에서 심사하는 시점의 랭킹을 기준으로 판정됩니다.
- 미등재 기업의 취약점을 제출할 경우, 해당 기업의 연락처를 함께 제출하는 것을 권장합니다.

포상금 기준

가상화폐 거래소

	High-risk	Mid-risk	Low-risk
1 등급(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
2 등급(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
3 등급(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
4 등급(DVP)	1000	500	200

거래소 등급 확인 사이트: https://www.coingecko.com/en/exchanges

1 등급 거래소 :

Binance	Huobi Global	FTX	OKEX
Bithumb	Upbit	Coinbase	BFX
Bybit	BitMex		

2 등급: Coingecko 거래소 랭킹 상위 20 위 중 1 등급 거래소를 제외한 거래소 (2 등급 거래소 중 DVP 기준보다 포상금이 높을 경우 초과된 금액은 화이트해커에게 추가 지급됩니다.)

3 등급 : 종합랭킹 상위 40

4 등급 : 종합랭킹 상위 40 이하

High-risk(높은 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

• 직접적으로 시스템 액세스 권한을 얻을 수 있음 ;

• 핵심업무의 심각한 디자인/로직 결함 ;

• 고객 및 기업 자산에 영향을 미칠 수 있음 (송금, 결제 /가상화폐 프라이빗 키 유출 등이 포함됨) ;

• 매수/매도를 작동시키는 불법적인 작동을 통하여 시장을 조작할 수 있음 ;

• 서버의 접근 권한을 직접 획득할 수 있음 ;

• 소스코드나 SQL 입력 등 대량의 민감한 정보를 직접적으로 탈취할 수 있음 ;

• interaction 없이 직접적으로 대량의 유저 정보나 서버관리 직원의 ID 를 도용할 수 있음. 사용자가 볼수 있는 페이지의 Stored XSS 혹은 관리자 서버에서 볼 수 있는 XSS 등 경우가 포함됨 .(서버 정보에 접근하여 정보를 탈취한 증명이 필요하며 증명하지 못할 경우 중간 또는 낮은 위험으로 분류 됨) ;

Mid-risk(중간 위험) :위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

• 일부분 사용자 정보 노출 등 소량의 민감한 정보 노출. SSRF 내부 네트워크 정보 노출 등이 포함됨 ;

• interaction 이나 익스플로잇을 통하여 사용자의 ID를 도용할 수 있는 취약점. 자주 사용하지 않는 페이지 Stored XSS, 관리자 서버에서는 보이지 않는 XSS 유형 취약점 등이 포함됨 ;

Low-risk(낮은 위험) : 실제 시도를 통한 성공 증명이 없이 이론만으로 가능함.

• 민감하지 않은 정보 노출. Directory Traversal 등이 포함됨 ;

• 실제 시도를 통한 성공 증명이 없이 이론만으로 가능함.

포상 대상에서 제외되는 경우 (DVP 입주 바운티 기업 제외):

• SPF mail forge 결함

• 이미 가입된 아이디 남용 문제 등

• 이용할 수 없는 self-xss / post 형 반사 XSS 상호작용의 요구가 높은 사용자의 아이디를 탈취할 수 있는 취약점. 반사형 XSS, 일반 CSRF 등이 포됨 ;

• URL Redirection ;

• 단문 메시지 인터페이스 남용 문제 등;

• 서비스 거부 결함

• 이메일 폭격

• 폐기된 사이트 혹은 스캠 사기 등 사이트 ;

• 본인 계정에만 영향주는 디자인 결함 및 로직 결함;

• 기타 실제 위협을 증명하기 어렵지만 이론상으로 존재하는 결함

블록체인/가상화폐

	High-risk	Mid-Risk	Low-risk
1 등급(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
2 등급(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
3 등급(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100

4 등급(DVP)	1000	500	200

랭킹 확인 사이트: https://coinmarketcap.com

1 등급 : 시총 랭킹 상위 10

2 등급 : 시총 랭킹 상위 20

3 등급 : 시총 랭킹 상위 40

4 등급 : 시총 랭킹 40 위 이하

Critical (심한 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 시스템 액세스 권한을 얻을 수 있음 ;
- 디지털 자산을 직접 탈취 할 수 있음 ;
- 심각한 민감한 정보 노출. 사용자의 프라이빗키, 비밀번호 등이 포함됨 ;

High-risk(높은 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 서비스 응답 거부로 이어질 수 있음 ;
- 다량의 사용자 / 거래소에 영향을 주는 디자인 결함 / 로직 결함 ;
- 디지털 자산을 추가 발행하거나 소각할 수 있음;
- 스마트 컨트렉트의 중요한 기능의 서비스 응답 거부 ;

Mid-risk(중간 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 로컬 권한 업그레이드로 이어질 수 있음 ;

- 사용자 본인 계정에만 영향을 주는 디자인 결함 / 논리적 결함;
- 간접적으로 높은 위협의 결함으로 이어질 수 있음 ;
- 일부 사용자의 디지털 자산을 추가하거나 소각할 수 있음. ;
- 스마트 컨트렉트내 혹은 사용자의 일부 자산을 제한적으로 탈취할 수 있음 ;

Low-risk (낮은 위험) :

- 일반 정보 노출 ;
- 낮은 위협의 디자인 결함 / 로직 결함 ;
- 시스템 자원 남용 또는 사용자 스팸을 일으킬 수 있는 루프 ;
- 이론상으로만 존재하는 결함. Owner 만 이용할 수 있는 결함 등이 포함됨.

지갑

	High-risk	Mid-risk	Low-risk
1 등급(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
2 등급(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
3 등급(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
4 등급(DVP)	1000	500	200

랭킹 확인 사이트: https://www.feixiaohao.com/wallet/

1등급 업체 :

TP	imToken	Math	Cobo

Trust	Metamask		

2 등급 : feixiaohao 사이트 랭킹 상위 10 위중 1등급 지갑을 제외한 기타 업체

3 등급 : 랭킹 상위 20

4 등급 : 랭킹 20 위 이하

Critical (심한 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 서비스 / 클라이언트 액세스 권한을 얻을 수 있음 ;
- 많은 양의 디지털 자산을 탈취할 수 있음 ;
- 심각한 민감한 정보 노출. 사용자 프라이빗 키/ 비밀번호 등이 포함됨 ;

High-risk (높은 위험) : 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 대량의 민감한 정보 노출 ;
- 서비스 / 클라이언트의 서비스 요청 거부;
- 많은 양의 사용자 ID 를 도용할 수 있음

Mid-risk (중간 위험) :위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 사용자 정보를 악의적인 변경할 수 있음
- 소량의 민감한 정보 노출
- 적은 양의 사용자 ID 를 도용할 수 있음

Low-risk (낮은 위험) :

- 일반 정보 유출 ;
- 실제 위협이 매우 낮은 디자인 결함 / 로직 결함 ;
- 시스템 정보 난용 또는 사용자 스팸을 일으킬 수 있는 루프

마이닝 풀

	High-risk	Mid-risk	Low-risk
1 등급(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
2 등급(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
3 등급(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
4 등급(DVP)	1000	500	200

랭킹 확인 사이트:https://btc.com/stats/pool?pool_mode=year

1 등급:

F2Pool	Binance Pool	Huobi.pool	AntPool
Spark pool			

2 등급: 랭킹 상위 10 위

3 등급: 랭킹 상위 15 위

4 등급: 랭킹 15 위 이하

Criciral (심한 위험)-위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 원격으로 마이닝 풀에서 모든 권한을 얻을 수 있음;
- 모든 마이닝 풀 계산 전력을 원격 제어 가능;
- 마이닝 풀 보상이나 지갑의 자산을 탈취할 수 있음;

High-risk (높은 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 마이닝 풀이 필히 이행해야 할 필수 서비스의 거부를 유도 할 수 있음;
- 블록 보류 공격, 컴퓨팅 파워 위조 등과 같은 마이닝 풀의 이자 손실로 이어질 수 있음;
- 대량의 민감한 정보 노출을 유도할 수 있음;

Mid-risk (중간 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

- 디자인 결함 / 로직 결함;

Low-risk (낮은 위험)- 실제 시도를 통한 성공 증명이 필요하지 않으며 이론만으로 가능

- 적은 양의 정보 노출로 이어질 수 있음;
- 특정한 조건 하에서만 실제 효과를 가질 수 있음

DEFI

	High-risk	Mid-risk	Low-risk
1 등급(USDT)	3000 ~ 5000	500 ~ 2000	50 ~ 500
2 등급(USDT)	1500 ~ 2500	250 ~ 1000	50 ~ 200
3 등급(USDT)	500 ~ 1000	100 ~ 500	50 ~ 100
4 등급(DVP)	1000	500	200

랭킹 확인 사이트: https://www.coingecko.com/en/defi (7 일 거래량 기준)

1 등급 : 랭킹 상위 10

2 등급 : 랭킹 상위 50

3 등급 : 랭킹 상위 200

4 등급 : 랭킹 200 위 이하

Critical (심한 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

• 계약을 탈취할 수 있거나 다른 사용자의 디지털 자산을 사용자의 의도 없이 계약할 수 있음;

High-risk (높은 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

• 디지털 자산을 만들거나 소각 할 수 있음;

• 계약의 중요한 기능이나 서비스 거부를 사용할 수 있음;

Mid-risk (중간 위험): 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함

• 일부 사용자의 디지털 자산을 추가하거나 소각 할 수 있음;

• 제한된 계약을 훔치거나 사용자의 디지털 자산을 사용자의 의도 없이 계약 할 수 있음;

Low-risk (낮은 위험): 실제 시도를 통한 성공 증명이 필요하지 않으며 이론만으로 가능

• 결함을 포함하여 이론적인 보안 결함은 소유자만이 악용할 수 있음.

위협 정보

	High risk	Medium risk	Low risk
1등급 (DVP)	3072	2048	1024
2등급 (DVP)	1024	512	256
3등급 (DVP)	512	256	128
4등급 (DVP)	256	128	64

High-risk (높은 위험) :

• 블록체인 관련 민감한 정보의 유출에 대한 명확한 증거;

•개인이 아닌 대량의 디지털 자산 절취와 관련된 확실한 증거;

• 블록체인 관련 미공개된 심각한 취약점 이용의 확실한 증거;

• 블록체인 산업에 관련 기업이 공격당한 내용과 이에 대한 증명이 가능한 경우;

• 블록체인 산업 관련 기업에게 큰 범위의 공격을 진행중인 내용과 이에 대한 증명이 가능한 경우;

• 블록체인 관련 소프트웨어/하드웨어에 부정한 수단이 있다는 증거를 제출하는 경우;

• 블록체인 산업 기업에 대한 새로운 공격 기술;

Mid-risk (중간 위험) :

• 블록체인 관련 취약점이 이용되고 있는 상황과 관련 증거가 있는 경우;

• 블록체인 보안 업계에 공개되지 않은 보안 사건 제보;

• 블록체인 기업에 관한 민감한 정보 유출;

Low-risk (낮은 위험) :

• 블록체인 산업에 포함된 기업의 낚시 사이트, App 등 제보;

• 블록체인 산업내의 불법 공격 관련 정보 제보.

비핵심 업무 취약점 기준

“비핵심 업무 취약점”이란 블록체인 기업의 주요 비즈니스와 관련이 없는 취약점을 뜻합니다.

예시: 블록체인/가상화폐 토큰, 지갑, DEFI 등의 홈페이지 관련 취약점.

만약 "비핵심 업무 취약점"이 주요 서비스에 영향 주게 되고 동시에 통용 규칙에 부합될 경우, 통용 규칙의 기준으로 포상금이 책정됩니다.

	High-risk	Low-risk
1등급 (USDT)	500 ~ 2000	50 ~ 500
2등급 (USDT)	250 ~ 1000	50 ~ 200
3등급 및 이하 (DVP)	500	100

1등급 : 메인 비즈니스 기준에서 랭킹 1등급 ;

2등급 : 메인 비즈니스 기준에서 랭킹 2등급 ;

3등급 및 이하 : 메인 비즈니스 기준에서 랭킹 3등급 및 이하 ;

High-risk (높은 위험):

- 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함;
- 원격으로 시스템 액세스 권한을 얻을 수 있으며 많은 양의 민감한 정보를 탈취할 수 있음(120 개 이상);
- 민감한 정보를 볼 수 있는 데이터 베이스에 액세스할 수 있음;

- 민감한 정보를 볼 수 있는 이메일에 임의로 접근할 수 있음;
- 사용자 혹은 기업에 큰 영향을 미칠 수 있음;

Low-risk (낮은 위험):

- 위험을 실현가능 하다는 이론이 아닌 실제 시도를 통한 성공 증명이 필요함
- Stored XSS, 관리자 권한 증명이 가능한 경우;
- 민감하지 않은 이메일에 접근할 수 있음;
- 중요하지 않은 데이터 베이스에 임의로 접근할 수 있음;
- 적은 양의 민감한 정보가 유출됨.

강등 규칙

- 포상금의 최종 표준은 취약점의 실질적 영향으로 미칠 수 있는 영향에 근거하여 책정됩니다;
- 위협 정도, 정보 탈취의 난이도, 영향 범위, 손실의 크기에 따라 판단이 되며;
- 실질적 영향이 매우 낮을 경우 DVP 에서는 아래의 강등 조건에 따라 포상금이 낮아질 수 있습니다.

강등 조건:

- 테스트 환경의 데이터 및 데이터의 양이 매우 적음;
- 운영되고 있지 않거나 버려진 사이트 등의 타깃일 경우;
- 취약점 이용 과정중에 일반 사용자외의 권한이 필요할 경우, 혹은 일정한 조건하에 만 해당 취약점의 포상금액이 강등 처리 됩니다;
- 동일한 타깃에서 여러 개의 취약한 비밀번호 취약점;

- 기타 DVP 펀드에서 강등으로 확정된 경우;
- 강등 범위는 최대 1등급을 초과하지 않습니다:
- 예시 1: 2등급 기업의 Mid-risk 취약점이 강등 될 경우 2등급 기업의 Low-risk 로 판정될 수 있고;
- 예시 2: 2등급 기업의 Low-risk 취약점이 강등 될 경우 3등급 기업의 Low-risk 로 판정될 수 있습니다.

"통용 취약점" 규칙

- 본 규칙은 DVP 플랫폼에 입주한 바운티 업체외의 기타 모든 업체에 적용됩니다.
- 취약점 자체는 가치가 없으며, 가치는 해당 취약점을 이용하여 발생할 수 있는 피해로부터 파생되므로 **취약점 포상액은 화이트 해커가 제보한 취약점 정보와 그 영향 범위와 정보 탈취의 난이도에 의해 결정됩니다. 참고: 기본적으로 심사위원은 취약점이 위험을 가져올 수 있다고 선입견을 가지고 있지 않으며, 실제 시뮬레이션과 같은 모든 증거는 취약점 정보 제출 시에 포함되어 있어야 하며 이론적으로 가능하다고 추측하는 정보는 유효하지 않습니다.**
- 버그 바운티 규칙에 적용되지 않는 취약점의 경우 DVP 가 상황에 따라 승인하거나 승인하지 않을 권한이 있습니다.
- 동일한 취약점이 서로 다른 타깃에서 발생하며 3 번 이상 제보된 경우 해당 유형의 취약점은 “통용 취약점 ”으로 중복 취약점으로 분류됩니다. 중복된

취약점으로 기록되지만 동시에 타깃 기업이 승인 여부를 결정할 수 있는 상태로 보류됩니다.

- 포상금 기준의 타깃(퍼블릭체인, 거래소 등)은 기업 자체의 서비스에 한정됩니다. 만약 타깃 기업의 산하 다른 자산(공식 홈페이지, 어플리케이션 등)에서 취약점이 발견된다면, 실제 영업 상황에 따라서 등급이 낮아집니다.
- “통용 취약점”을 제보할 경우 해당 취약점이 발생하는 타깃 업체의 정확한 주소를 명시해야 하며 최소 5개 이상의 유효 타깃을 포함해야 합니다.
- “통용 취약점”을 제출할 경우 해당 취약점이 발생하는 기업중에 등급이 높은 기업을 기준으로 책정됩니다. 상위 3개의 기업은 일반적인 버그 바운티 규칙에 따라 각각 포상금이 지급되는것 외에 추가적으로 상위 3개 기업의 취약점 포상금의 평균 포상금이 지급됩니다. 즉 최종 포상금= 기업 등급이 상위 1.2.3 기업의 포상금 +3개 기업의 포상금 총합/3. 참고:1등급 입주 기업의 포상금만 기업에서 수령하지 않았을 때 재단에서 대신 지급하고, 기타 등급의 기업은 수령 확인 후 기타 포상금을 화이트해커에게 지급합니다.
- 동일한 취약점 소스에서 발생한 여러개의 취약점은 하나로 간두됩니다. 예를 들어 동일한 인터페이스로 인한 여러개의 취약점; 동일한 게시 시스템으로 인한 여러 페이지 보안 결함, 전체 사이트 보안 결함을 유발하는 프레임 워크, 범용 도메인 해석으로 인한 여러 보안 취약점; 기업에서 신분 검증을 하지 않음으로 유발한 시스템의 여러 인터페이스 월권 혹은 token 검사를 하지 않아 발생한 여러 CSRF 취약점; 동일한 파일과 같이 동일한 소스에서 나온 결함 등은 하나의 취약점으로 취급됩니다.

- 인터페이스 남용/문자 메시지 폭격, API 문서 유출, URL Redirection , 반사형 XSS, DOM-Based XSS , 실현 요구가 높은 CSRF/JSONP Hijacking/CORS 민감정보 등 위험성이 낮은 취약점은 수령 범위에 속하지 않습니다.
- OSS/Bucket 등에 업로드 되는 Stored-XSS 는 실제 취약점의 위험 정도에 따라 강등되거나 거절됩니다.
- 일부 서비스 거절 취약점 (예시: 동일한 타깃에 대량의 공격을 실행하여 서버가 늦어지는 경우, 사이트가 열리지 않는 경우등) 은 수령 범위에 속하지 않습니다.
- 이용 난이도가 높은 사용자의 일부 정보 유출 혹은 디자인 결함은 취약점 수령 범위에 속하지 않습니다.
- 타깃 서비스에 포함되어 있는 타사 제품 예를 들어서 WordPress, Flash, Apache , OpenSSL, SDK 등등 여러가지 소프트웨어 버전의 동일한 곳의 취약점은 한개의 취약점으로 간주됩니다.
- 같은 취약점이지만 2 명이 제보할 경우 이후에 제출 된 취약점 이용 방법이 첫번째 제출한 이용 방법과 차이가 클 경우, 2 개의 취약점 모두 심사에 통과되지만 이후 제출 된 보상의 일정 부분이 첫 번째 제출자에 지급됩니다.
- 제출자는 DVP 에 이미 제보한 취약점을 다른곳에 공개하거나 타 플랫폼에 취약점 정보를 게시하거나 제출할 수 없습니다. DVP 에서 부정행위를 발견할 경우 계정과 자산이 동결될 수 있습니다.
- 취약점 이용 과정중에 일반 사용자외의 권한이 필요할 경우, 혹은 일정한 조건하에 만 유발되는 취약점은 포상금액이 강등 처리 됩니다.
- 취약점 통합

- 전후 관계가 있는 1개 이상의 취약점은 취합하여 1개의 취약점으로 처리될 수 있으며 심사 결과에 따라 포상금은 높아질 수 있습니다. (예시: 백엔드 시스템에 들어갈 수 있는 취약점을 제보했다가 백엔드에서 SQL injection 취약점이 발생하는 경우) 이미 제보한 취약점에 관하여 추가적인 정보를 취득하였을 경우 해당 내용을 보충하여 더 높은 포상금을 받을 수 있습니다.

- 하나의 취약점을 여러개로 나누어서 제출하는 경우, DVP는 이들을 하나로 통합하여 처리할 수 있으며 포상금은 그 중 최고 등급 기준으로 책정됩니다. 제출자가 악의적으로 취약점을 분할하여 제보할 경우 DVP에서는 악의적인 행위에 대한 확인을 거친 후 계정을 동결할 수 있습니다.

- 다음과 같은 경우 제출자의 계정과 자산이 동결될 수 있습니다:

- 순서가 지정된 취약점에 대해 가장 마지막 순서의 취약점을 먼저 제출합니다. 예를 들어서 이메일 주소의 취약점을 발견하고 해당 이메일을 통하여 백엔드 관리자 계정을 탈취할 수 있지만 백엔드 탈취 부분을 먼저 제출하고 이메일 취약점을 나중에 제출하는 경우입니다.

- 취약점 테스트를 빌미로 발견한 취약점을 이용하여 사용자의 이익에 해를 끼치고 사용자의 비즈니스에 영향을 미치면 DVP는 포상금을 지급하지 않으며 해당 계정 및 자산을 동결할 수 있습니다.
- 등재되지 않은 기업의 취약점에 대해서는 DVP 재단에서 일시 기각 처리하고, 적합시에는 해당 업체의 취약점을 수록 개시 하며, 중복 취약점이 있는 경우에는 수록 개시 후 선착순 제출을 기준으로 이전 기각된 취약점을 재제출할 수 있도록 하는 것이 원칙입니다.

- 명확한 설명이 없는 제출물의 경우 즉시 거부됩니다. 모든 취약점 제보에는 타깃 URL(웹사이트일 경우), 텍스트 세부 정보, 이미지 파일 및 명확한 설명 포함됩니다. 예를 들면:

- 타깃 기업의 웹 사이트 주소, 웹 사이트 주소가 없을 경우 별도의 설명이 필요합니다.
- 상세 정보에는 취약점과 관련된 모든 URL 이 포함되어야 합니다.
- 취약점 증명시 모든 주요 단계를 나열해야 하며, 이는 심사위원이 추측이 아닌 오로지 제출된 설명에 근거하여 재현할 수 있어야 합니다.
- 취약점 관련 payload 는 상세 정보 텍스트에 입력해야 하며 스크린 샷으로만 제출해서는 안 됩니다.
- 운영되고 있지 않거나 버려진 사이트 등의 타깃일 경우;
- GitHub 정보 노출, memcache, redis unauthorized access 등과 같은 정보 노출 유형 결함은 내용의 타당도 및 민감도에 따라 분류되며 격리 및 위험도가 낮은 노출은 무시할 수 있습니다.
- 백엔드 취약점의 문제는 성공적인 탈취의 증거가 있어야 하며 그렇지 않을 경우에는 거부됩니다.
- 취약한 비밀번호 문제 (정상적으로 대외 가입이 가능한 시스템 제외):

- 동일한 제출자가 발견한 동일한 시스템의 서로 다른 취약한 비밀번호는 하나의 사례로 간주됩니다. (만약 기업에서 이전의 취약 비밀번호을 처리한 경우, 2 차 제출 시 강등 처리되고 2 차 이후에 제출하는 것은 모두 병합 처리됩니다).

- 기본 초기 비밀번호는 하나의 사례로 간주됩니다. (예를 들어 이메일의 초기 비밀번호는 모두 동일한 비밀번호일 시 하나의 취약점으로 간주됩니다.)

- 중요하지 않은 시스템의 경우 첫 번째 제출 된 취약한 비밀번호 취약점만 승인됩니다.

- 필수 시스템 및 핵심 비즈니스의 경우, 순서대로 첫 2개의 취약점이 승인됩니다.

- 전후 관계가 있는 연결성 취약점의 경우 여러 사례로 분할하여 제출시 악의적인 경우 DVP에서 해당 계정을 동결할 수 있습니다.
- IIS 서비스 거부 또는 slow_http_dos 등과 같은 서비스 중단을 유발할 수 있는 테스트를 실행하면 안됩니다.
- 서비스에 PC 사이트와 모바일 웹 사이트가 모두 있고 동일한 인터페이스와 소스 코드를 사용하는 경우 PC/App/ 사이트의 동일한 결함으로 취급되며 주동적으로 통합하여 제보할 경우 상황에 따라 포상금이 높아질 수 있습니다. 다른 제보자가 제출할 경우 타깃 기업이 해당 취약점을 패치하기 전에는 중복된 취약점으로 취급됩니다.
- 정보 유출의 취약점에 관해서는 실제 탈취 후 피해 사례가 발생할 수 있는 제출물은 심각하거나 높은 위험으로 간주됩니다. 주요 서비스 구성 또는 소스 코드 노출은 중간 위험으로 간주되고 이용하기 어렵거나 또는 핵심 비즈니스와 관련이 없으며 낮은 위험 또는 거부할 수 있습니다.

공급업체 보호

하나의 시스템에서 동일한 유형의 높은 위험 결함(예: SQL injection 등)이 3 개 이상 발견되면 심사위원은 해당 시스템이 보호 기능이 없다고 간주하고 이후에 제출된 동일 유형의 취약점은 강등 처리 됩니다.

취약점 심사 분쟁

취약점 보고서 처리 과정에 제보자가 만약 처리 과정 , 취약점 등급, 포상금 지급 등에 관하여 의견 충돌이 있을 경우 취약점 상세 페이지에서 메시지를 남기거나 DVP 담당 직원에게 연락하여 의의를 제기할 수 있습니다. DVP 는 취약점 제보자의 이익을 최우선으로 하는 원칙으로 바운티 제공 업체와 적극적으로 협상할 것이며 필요할 경우 보안 업계의 제 3 자 기업들을 동원하여 공정한 결과를 발표하도록 할 것입니다.

참고

본 버그 바운티 규칙은先知众测漏洞定级标准제 3 의 사이트 버그 바운티 플랫폼 취약점 등급 기준을 참고로 작성되었습니다.