



하이콘 바운티_{코드} 프로그램 가이드라인

001C 출시

Developer



목차

1. 소개	3
1.1 목적	3
1.2 문서 작성 규칙	3
1.3 프로젝트 참조 자료	4
2. 바운티 프로그램 & 규칙	5
2.1 바운티 프로그램 소개	5
2.2 규칙	5
3. 참여 방법	7
3.1 범위	7
3.2 이슈 보고	7
3.3 풀 리퀘스트	7
3.4 하이콘의 사용자 지정 프로젝트	8
4. 보안 버그 / 취약점	9
4.1 절차	9
4.2 카테고리	9
4.3 정보 공개	9
4.4 공식 인정	9
4.5 가이드라인	10
5. 제출 절차 & 법률 정보	11
5.1 제출 절차	11
5.2 법률 정보	11
6. 부록	12
6.1 보안 이슈 범위	12
7. 수정 기록	12
업데이트 내용	12

Commented [윽1]: There's also 4.5 가이드라인

1. 소개

1.1 목적

본 서류는 하이콘 바운티 프로그램의 설명서로서 하이콘 프로젝트에 기여하기를 원하는 개발자들을 위해 만들어진 가이드라인이다. 개발자 (이하 '기여자'로 표기)는 하이콘 프로젝트와 관련된 문제 사항을 보고하거나 개선점을 제안하고 HYC 를 받을 수 있다.

“필독”: 본 서류는 추후 수정되거나 업데이트 될 수 있다.

1.2 문서 작성 규칙

글로스퍼 (Glosfer), ㈜ 글로스퍼 (Glosfer corp.), 인피니티 블록체인 (Infinity Blockchain), 하이콘 (Hycon), HYC 와 ㈜ 글로스퍼 등록 상표는 모두 기업명 ㈜ 글로스퍼와/또는 하이콘 프로젝트를 지칭한다. 위에 언급된 상호명은 상호 호환하여 사용할 수 있다.

바운티 프로그램 (Bounty program), 바운티 (Bounty), 코딩 기여 프로그램 (Coding Contribution program), 그리고 코딩 기여 (Coding Contribution)는 모두 하이콘 프로젝트의 바운티 프로그램을 지칭한다. 위에 언급된 단어는 상호 호환하여 사용할 수 있다.

“반드시, 의무적인, 금지된, 필수, 추천하는, 추천하지 않는, 제안되는, 가능성이 있는, 선택적인, 구성하는, 포함하는” 등의 표현을 사용하면 아래와 같은 의미로 해석한다.

- “반드시, 요구되는, 의무적인”은 해당 문장이 절대적이라는 뜻이다.
- “금지된” 또는 “~하면 안되는”은 해당 문장이 절대적으로 금지되었다는 뜻이다.
- “~해야 한다” 또는 “제안되는”은 해당 문장의 방향을 결정하기 전에 전제 조건 및 합의가 이해되어야 한다는 뜻이다.
- “할 수 있는, 선택적인”은 해당 문장이 절대적으로 선택 사항이라는 뜻이다.
- “대체로”는 해당 문장에 묘사된 행동이 추측되는 행동이며 이와 같은 행동이 일어날 가능성이 높다는 뜻이다.
- “~로 이뤄지다”란 문장에 기입된 모든 요소, 또는 기입되지 않은 요소가 모두 포함되어 있다는 뜻이다.
- “~로 구성하다”는 문장에 기입된 모든 요소가 모두 포함되어 있으며 기입되지 않은 요소는 포함되어 있지 않다는 뜻이다.

1.3 프로젝트 참조 자료

[GitHub Guides](#)

[GitHub Labels - HYCON core](#)

[OWASP risk rating model](#)

[CVE - Common Vulnerabilities & Exposures](#)

2. 바운티 프로그램 & 규칙

2.1 바운티 프로그램 소개

하이콘의 바운티 프로그램은 매우 광범위한 프로그램이다. 이는 컨센서스 모델, p2p 프로토콜, 작업 증명 등과 같은 시행 준수 사항부터 네트워크 보안과 합의 무결성까지 포함한다. 이 프로그램은 실험용으로 제량에 따른 보상을 지불함으로써 하이콘 커뮤니티의 서포터들이 하이콘 플랫폼 개선에 기여할 수 있도록 돕는다. 하이콘 [GitHub](#) 와/또는 security@glosfer.com 로 코드와 관련된 수정사항 및 개선점을 제출할 수 있다.

2.2 규칙

2.2.a 일반 규칙

참여 전 확인 사항

- 제출된 적 있는 제출 작품, 혹은 이미 클레임이 진행되고 있거나 제출되어 프로세스가 완료된 제출 작품은 보상받을 수 없다.
- 하이콘 연구팀이 이미 인지하고 있는 이슈 및 풀 리퀘스트(Pull Request) 제출은 보상받을 수 없다.
- 승인된 *Note reward-size* ([2.2.b Reward Sizes](#) 참조) 의 풀 리퀘스트는 유저 당 한달에 한번만 수락한다. ([3.3 Pull Requests](#) 참조)
- 공개된 취약성 정보는 바운티에 참여할 수 없다. ([4 Security Bugs](#) 참조).
- 버그 헌팅을 위해 프라이빗 체인을 시작하거나 포크를 진행한다. 메인 및 테스트 네트워크를 공격하지 않도록 조심한다.
- 하이콘 및 ㈜글로스퍼의 연구팀, 개발팀, 임직원 및 직, 간접적으로 당사에 취업하고 있는 모든 이들은 바운티를 통해 보상을 받을 수 없다.
- 보상의 크기는 여러가지 변수에 의해 결정된다. 적격성, 점수 및 버그와 관련된 모든 사안과 취약성, 그리고 보상의 크기 결정과 관련된 최종 권한은 바운티 프로그램팀이 갖는다.

이슈와 관련된 보상은 **심각도**에 따라 다르다. 심각도는 “영향력과 가능성”에 따라 [OWASP](#) 위험도 평가 모델에 의해 결정된다.

		Likelihood		
		Low	Medium	High
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Severity		

심각도 외에도 다음과 같은 기타 변수들이 고려된다:

- 작품의 품질. 의미가 분명하고 잘 쓰인 제출 작품에는 더 큰 보상이 주어진다.
- 재현성의 품질. 테스트 코드, 스크립트, 상세 지침을 포함하면 대응 속도가 개선된다.
- 수정의 품질(적용 가능할 때). 솔루션이나 이슈 수정 방법 등에는 더 큰 보상이 주어진다.

바운티 보상에 영향을 미치는 다른 이슈들에 대해 알고 싶으면 [5.2 법률 정보](#)를 참조한다.

2.2.b 보상 크기

보상 크기는 아래 규칙을 따르지만 최종 결정권은 바운티 팀에게 있다.

- **크리티컬:** 바운티 팀에게 연락
- **높음:** 최대 \$5,000
- **중간:** 최대 \$1,000
- **낮음:** 최대 \$500
- **노트:** 최대 \$100

수정이나 패치가 포함된 제출 작품은 최초 보상 크기의 100%에 해당하는 추가 보상을 받을 수 있다.

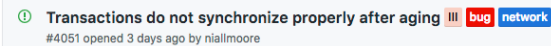
3. 참여 방법

3.1 범위

이 장에서는 기여자를 위한 가이드라인, 프로세스, 규격화된 정보를 제공한다. 버그 헌팅과 보고 활동은 [깃허브 저장소](#)와 security@glosfer.com에서 이루어진다.

3.2 이슈 보고

“필독”: 깃허브 관련 이슈에 대한 자세한 설명은 [Mastering Issues](#)에서 확인할 수 있다.



① Transactions do not synchronize properly after aging **bug** **network**
#4051 opened 3 days ago by niallmoore

Figure 1 | 이슈의 예시

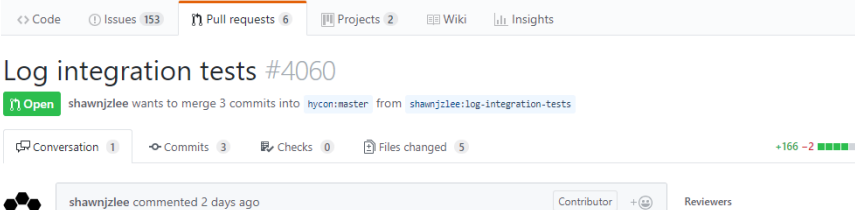
기여자는 이슈를 저장함으로써 작업물, 개선점, 버그 등을 기록할 수 있다. 이러한 이슈는 공개적으로 공유되어 논의된다. **이곳에 취약성과 관련된 사항을 절대 누설해서는 안된다.**

해당 바운티는 아래와 같은 이메일 형식을 취해야 한다.

- ID#: 이슈 ID 넘버
- 깃허브 사용자 명
- 하이콘 지갑 주소
- 이슈에 대한 짧은 요약 및 설명
-

3.3 풀 리퀘스트

“필독”: 깃허브의 풀 리퀘스트에 대한 자세한 사항은 [About pull requests](#)에서 확인할 수 있다.



<> Code ① Issues 153 Pull requests 6 Projects 2 Wiki Insights

Log integration tests #4060

shawnjzlee wants to merge 3 commits into hycon:master from shawnjzlee:log-integration-tests

Conversation 1 Commits 3 Checks 0 Files changed 5 +166 -2

shawnjzlee commented 2 days ago Contributor Reviewers

Figure 2 | 풀 리퀘스트 예시

기여자는 모든 사용자를 위해 코드베이스를 향상할 수 있는 풀 리퀘스트를 제출할 수 있다. 하이콘은 코드베이스에 의미 있는 변화를 줄 수 있는 모든 풀 리퀘스트를 환영한다. 이는 유형 수정부터 번역 도움(번역의 경우 “노트” 보상 크기), 코드 준수와 완결성까지 포함한다.

풀 리퀘스트는 다른 사용자의 이슈(들)를 참고하여 만들 수 있다. 이와 같은 바운티의 경우, 아래와 같은 형식의 이메일을 제출한다.

- 개인 정보
 - o 기트허브 사용자 명
 - o 하이콘 지갑 주소
- 풀 리퀘스트 정보
 - o 풀 리퀘스트 ID 번호
 - o 관련 이슈의 ID 번호 (해당 시)
 - o 실행한 풀 리퀘스트의 요약
 - o 요건과 시험 사례 (해당 시)

3.4 하이콘의 사용자 지정 프로젝트

하이콘의 주요 철학 중 하나는 사용 및 개발이 용이한 생태계의 구축이다. 사람들이 아이디어를 제출하면 하이콘 팀이 검토해서 구체화시키는 것이다. 아래 유형의 테고리를 제출할 수 있으며 여기에 포함되지 않은 카테고리의 제출도 환영한다.

- API 통합
- 상업적 플러그인
- 게임
- 하드웨어 통합
- 하이콘 관련 앱

사용자 지정 프로젝트는 MIT 라이선스를 준수해야 하며 다른 바운티 보상과 중복 적용될 수 없다. 자세한 정보는 security@glosfer.com 으로 문의 가능하다.

바운티 프로그램에 참여하려면 아래 형식의 이메일을 제출해야 한다.

- 개인/팀 정보
 - o 이름, 기트허브 사용자 명, 거주 국가
 - o 하이콘 지갑 주소
- 사용자 지정 프로젝트 정보
 - o 프로젝트 카테고리
 - o 타임라인 / 소요 시간
 - o 프로젝트/사업계획 요약 (큰 프로젝트에 한함)

4. 보안 버그 / 취약점

4.1 절차

보안 이슈는 폴 리퀘스트와 비슷하지만 보안상의 이유로 security@glosfer.com 로 제출되어야 한다. 제출된 보안 이슈는 일반에 공개되지 않으며 완료될 때까지 이메일로 모니터링된다.

이 정보는 바운티 팀의 허락을 받아 기여자 측의 도메인 전문가들과 공유할 수 있다. 허락 조건은 대중에게 공개하지 않는 것과 취약성 관련 커뮤니케이션 시 security@glosfer.com 을 수신자 목록에 포함하는 것이다.

정보를 대중에 공개한 기여자는 블랙리스트에 오르게 된다.

4.2 카테고리

바운티 코드 프로그램의 범위에 따르면 한 개 이상의 카테고리가 보안 이슈에 해당된다. 보안 이슈가 구체적 CVE 에 해당한다면, 기여자는 한 개 이상의 이슈 관련 CVE 번호를 제공해야 한다. 그 외의 경우는 [6.1 보안 이슈 범위](#)를 참조한다.

4.3 정보 공개

취약성 보고서는 처음에는 비공개 상태로 유지되어 수정사항 발표에 필요한 충분한 시간을 보장한다. 아래는 공개 옵션들이다:

- **기본 옵션:** 하이콘 담당자나 기여자가 이의를 제기하지 않을 경우, 보고서는 30 일 이내에 대중에 공개된다.
- **상호 동의:** 하이콘 담당자와 기여자간에 상호 동의한 타임라인을 생성할 수 있다. 단, 타임 라인 관련해서 개방된 의사소통이 이루어져야 한다.
- **연장:** 취약성 관련 복잡성 및 기타 요소들로 인해 수정에 더 많은 시간이 필요할 경우, 하이콘 담당자가 타임라인 연장 요청을 해야 한다.

4.4 공식 인정

기여자가 아래 조건을 충족할 시, 공식 인정을 받을 수 있다:

1. 기여자가 해당 취약성의 발견자일 때
2. R&D 팀이 취약성을 타당한 보안 이슈로 인정했을 때
3. 기여자가 정확한 계정 정보와 취약점 해결을 위해 이루어진 대화 내용을 제공했을 때
4. 기여자가 위 가이드라인을 모두 준수했을 때 ([4.1](#), [4.2](#), [4.3](#))

하이콘은 위 조건을 충족한 모든 사람에게 발견 이슈, 해결책, 경험을 원하는 형태로 공유할 것을 권한다.

4.5 가이드라인

각 바운티는 아래의 제출 형식을 갖춰야 한다:

- 개인 정보
 - o 기여자의 이름 혹은 가명
 - o 거주 국가
 - o 하이콘 지갑 주소
- 풀 리퀘스트 정보
 - o CVE ID(해당될 경우)
 - o 작업 범위(해당될 경우, [6.1 보안 이슈 범위](#) 참조)
 - o 관련 있는 가장 최근 출시 버전
 - o 시행 내용 상세 요약
 - o 시험 요건 및 시험 사례

5. 제출 절차 & 법률 정보

5.1 제출 절차

하이콘의 바운티 프로그램은 이슈 발견, 풀 리퀘스트, 사용자 지정 프로그램, 취약점 발견등에 대한 대가로 금전적 보상을 제공한다. 모든 기여자에게 보상이 주어지는 것은 아니며 보상 관련 결정은 바운티 팀에 의해 내려진다. 각 제출 작품에 지불되는 보상의 액수 또한 바운티 팀에 의해 결정된다. 각 보상은 독립적으로 이루어지며 서로 영향을 주지 않는다. 보상 조건에 대한 협상은 따로 이루어지지 않는다.

노트 보상 크기 제출 작품은 기트허브 사용자 별로 한달에 한번씩 확인된다. 한달간 제출한 작품들을 모아 놓으면 효율적 확인에 도움이 된다.

매월 첫 화요일에 전달 제출, 취합된 제출 작품들에 대한 보상이 지급된다. 지급 전 바운티 팀 매니저가 기여자에게 연락을 취할 것이다. 제출 관련 질문에 대한 답변은 3 근무일 이내에 처리된다.

5.2 법률 정보

보상을 받으려면 다음의 자격조건을 충족해야 한다:

- 대한민국과 거래 제한이나 수출 금지 관계에 있는 국가의 기여자는 바운티를 지급받을 수 없다.
- 채굴자들도 참여할 수 있다. 다만 바운티 지급은 채굴자의 부모님이나 법적 대리인에 의해서만 수령 가능하다.
- 모든 바운티는 지급시 미 달러 시세에 맞춰 하이콘으로 지불된다. 따라서 바운티 보상을 받으려면 하이콘 지갑을 가지고 있어야 한다.
- 모든 보상은 관련 법과 세금제도를 준수해야 한다.
- 기여자가 만든 테스트는 법을 위반하거나 타인의 데이터를 손상시켜서는 안 된다.

6.부록

6.1 보안 이슈 범위

6.1.a 프로토콜 보안

6.1.b 실행 보안

클라이언트 애플리케이션 보안

클라이언트 프로토콜 실행

암호 원시 요소 보안

데이터베이스 실행

데이터베이스 보안

네트워크 보안

노드 보안

7. 수정 기록

이 장은 하이콘 바운티 가이드의 수정 기록이다.

업데이트 내용

- 2018/06/29_19:19 - 리뷰 및 제안 접수. 사용자 지정 프로젝트 및 취약점 관련 이메일 가이드라인 추가. 오타 수정.
- 2018/06/29_16:39 - 소개, 규칙, 제출 방식, 법률 정보 란 수정.
- 2018/06/04_00:00 - 바운티 코드를 제외한 가이드 초안.