

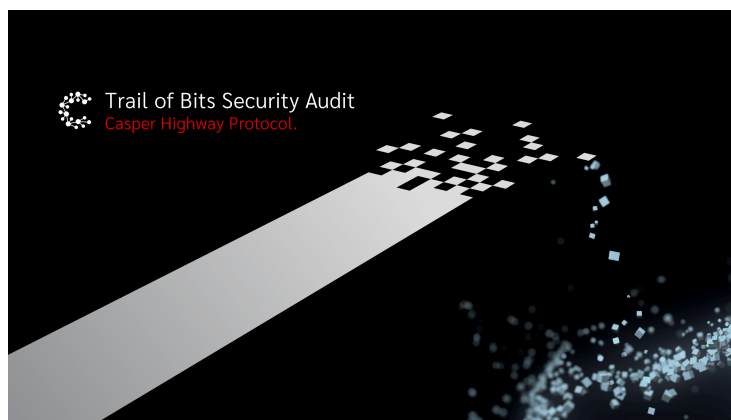
[Trail of Bits citation guidelines](#)  
[Trail of Bits 인용 가이드라인](#)

<Title> Trail of Bits has Completed an Audit of the Casper Highway Protocol

Trail of Bits를 통해 캐스퍼 하이웨이 프로토콜 감사가 완료되었습니다

<Subtitle> An overview of the December 2020 audit of Casper’s Highway Protocol completed by Trail of Bits.

Trail of Bits가 완료한 캐스퍼 하이웨이 프로토콜에 대한 2020년 12월 감사 개요입니다.



Published today, Trail of Bits has completed an audit of the Casper network Highway Protocol. The Trail of Bits audit “did not produce high severity results and showed proper use of security hygiene.”

오늘 게시된 바와 같이 Trail of Bits는 캐스퍼 네트워크 하이웨이 프로토콜의 감사를 완료했습니다. Trail of Bits 감사는 “심각도가 높은 결과를 생성하지 않았으며 보안 위생의 적절한 사용을 보여주었습니다.”

[<View the Audit>](#)  
[<감사 내용 보기>](#)

## Engagement Scope

감사 범위

The Trail of Bits audit was completed between November 16th and December 1st, and encompassed an assessment of CasperLabs’ Highway consensus protocol. The audit sought to answer critical questions, including:

Trail of Bits 감사는 11월 16일과 12월 1일 사이에 완료되었으며 캐스퍼랩(CasperLabs)의 하이웨이 컨센서스 프로토콜에 대한 평가 또한 여기에 포함되었습니다. 감사를 통해 다음과 같은 중요한 질문에 답을 찾고자 했습니다.

- Will misbehaving validators be punished?
- 부정 행위를 하는 검증자는 처벌을 받습니까?
- Is the system prone to a resource exhaustion attack?
- 시스템이 리소스 소모 공격에 취약합니까?
- Are units appropriately validated before being appended to state?
- 유닛들은 스테이트에 첨부되기 전에 적절하게 검증이 되고 있습니까?
- Can an attacker game the system such that they are selected as the next leader?
- 공격자가 다음 리더로 선정되도록 시스템에 대해 게임을 할 수 있습니까?
- Is LNC validation appropriately implemented? Is the buffer mechanism for LNC validators appropriate?\*
- LNC 검증이 적절하게 구현되어 있습니까? LNC 검증자의 버퍼 메커니즘이 적절합니까?\*

\*LNC is “Limited Naivety Criterion.” Learn more in the [Casper Highway Protocol paper](#).

\*LNC는 “Limited Naivety Criterion”의 약자입니다. [캐스퍼 하이웨이 프로토콜 문서](#)에서 자세한 정보를 확인할 수 있습니다.

## Engagement Findings

감사 결과

The security audit yielded three findings, 1 of “informational severity” and 2 of “low severity.” 보안 감사를 통해 “정보적 심각도” 1개와 “낮은 심각도” 2개로 총 세 가지 결과가 나왔습니다.

- LNC validation not implemented (informational severity)
- LNC 검증이 구현되지 않음 (정보적 심각도)
- Peers are not punished for sending invalid vertices (low severity)
- 피어가 유효하지 않은 정점을 보낸 것에 대해 처벌을 받지 않음 (낮은 심각도).
- Insufficient rate limiting mechanism (low severity)
- 불충분한 속도 제한 메커니즘 (낮은 심각도)

In addition, the Trail of Bits team offered recommendations to improve the clarity and detail of portions of the Highway Protocol documentation itself.

또한, Trail of Bits 팀은 하이웨이 프로토콜 문서 자체의 일부의 명확성과 세부 사항을 개선하기 위한 몇 가지 권장 사항을 제안했습니다.

## CasperLabs’ Fix Log

캐스퍼랩 수정 로그

CasperLabs received and reviewed the Trail of Bits audit, and made changes to the three findings.

캐스퍼랩(CasperLabs)은 Trail of Bits 감사를 받고 검토했으며 다음의 세 가지 결과에 대해 변경 조치를 했습니다.

- LNC validation not implemented. **Fixed.**
- LNC 검증이 구현되지 않음. 수정됨.
  
- Peers are not punished for sending invalid vertices. **Partially Fixed.** The risk associated with this issue is noted as very low in practice.
- 피어가 유효하지 않은 정점을 보낸 것에 대해 처벌을 받지 않음. 부분적으로 수정됨. 해당 문제와 관련된 위험은 실제로 매우 낮습니다.
  
- Insufficient rate limiting mechanism. **Partially Fixed.** The risk associated with this issue is noted as very low in practice.
- 불충분한 속도 제한 메커니즘. 부분적으로 수정됨. 해당 문제와 관련된 위험은 실제로 매우 낮습니다.

The CasperLabs team also adjusted the relevant portions in the protocol paper pointed out by the Trail of Bits security audit as needing improvement.

캐스퍼랩 팀은 또한 Trail of Bits 보안 감사에서 개선이 필요한 것으로 지적된 프로토콜 문서의 관련 부분을 변경했습니다.

CasperLabs thanks the Trail of Bits team for the engagement and audit.

캐스퍼랩은 Trail of Bits 팀의 헌신적인 감사 활동에 감사한 마음을 전합니다.

[<View the Audit>](#)

[<감사 내용 보기>](#)