Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Consulting-Report Ethereum Discv5 12.2019 - 01.2020

Cure53, Dr.-Ing. M. Heiderich, Prof. N. Kobeissi

Index

Introduction

“Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.”

From https://ethereum.org/

This report documents the results of a consulting exercise completed by Cure53 for the Ethereum (ETH) team. The project was carried out in December 2019 and January 2020 and mostly focused on the Ethereum Node Discovery Protocol v5.

In terms of resources, Cure53 was awarded a pool of ten days that could be used for testing. To date, five days have been used by two members of the Cure53 team involved in this exercise. This means that there is a remaining budget of five days that can still be allocated by Ethereum to further work.

To make sure that the exercise fits in with the goals and interests of Ethereum, the consulting work was accompanied by a kick-off, several meetings and communications enabled by the Discord server maintained by the Ethereum team, specifically through a dedicated channel (*#discv5*) that was opened for the purpose of sharing exercise-related details. The two members of the Cure53 joined the channel, yet it should be stated that one had a managerial and administrative role, while the other performed the tasks related strictly to the consulting and analysis.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

In terms of approaches, the analysis centered on the Discv5 protocol, which is used to establish decentralized handshakes between nodes. The protocol had already been audited in the past and comes as the fifth iteration of the ETH discovery protocol framework. As part of the audit, the protocol's handshake and wire format were both subject to formal evaluation. This also included exotic XOR-based constructions that the ETH team noted as needing particular attention.

The findings encompass two items marked with corresponding severity levels which denote impact of the findings for the connected implementation. These outcomes take on a case of the protocol being rolled out 'as is'. While one concern has only *Informational* character, the other was evaluated as *Medium* because of the shortcomings affecting mutual authentication for the bootstrapping nodes.

The following sections will first report on the consulting scope and information shared with Cure53 prior to the beginning of the engagement and aimed at supporting analytical tasks. Next, the concerns and observations pertinent to the scope and discussed with the Ethereum team are documented by Cure53 in a chronological order. The report will then close with a brief conclusion in which the results of this consulting exercise are summarized alongside high-level advice for possible hardening and reinforcement of the existing security guarantees.

Scope

- **Consulting on Ethereum Node Discovery Protocol v5**
  - https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md
  - https://github.com/ethereum/devp2p/blob/master/discv5/discv5-wire.md#handshake

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Miscellaneous Issues

This section covers those noteworthy findings that did not lead to an exploit but might aid an attacker in achieving their malicious goals in the future. Most of these results are vulnerable code snippets that did not provide an easy way to be called. Conclusively, while a vulnerability is present, an exploit might not always be possible.

ETH-06-001 Protocol: Limitations in noderecord directory authentication *(Medium)*

It was found that the bootstrapping procedure that the Discv5 nodes rely on fails to provide any mutual authentication with regards to the bootstrapping nodes. If the initial bootstrap nodes are compromised, all future decentralized network interaction by the victim's nodes would be controlled by the attacker.

The Discv5 designers are aware of this risk and propose using Node Discovery Via DNS (EIP-1459)[1] as a potential remedy for the issue. In the case of EIP-1459 deployment, root-signing key communication becomes critical. Therefore, it is best to ship it hard-coded within Discv5 clients, with rigid rekeying protocol requirements.

ETH-06-002 Protocol: Pre-shared key support considerations *(Info)*

The decentralized use-case for Discv5 cannot be realistically paired with mutual authentication based on long-term keys. However, it is recommended to investigate supporting pre-shared key (PSK) features, which could allow nodes to optionally instantiate authenticated connections. This calls for both providing a matching pre-shared symmetric key. Such features are available in TLS 1.3, where they are used for session resumption[2] and in the Noise Protocol Framework, which employs them to improve the authentication security properties of sessions[3].

Further comparisons have been drawn between Discv5 and certain Noise Handshake Patterns, such as NK[4] or IK[5]. According to the Discv5 designers, the main reason for reticence regarding the use of the Noise Protocol framework stemmed from uncertainty as to whether session IDs can be included within the wire protocol. Despite this, session IDs and other Discv5-relevant materials can be included within a custom data serialization format within the Noise Handshake Protocol payloads.

[1] https://eips.ethereum.org/EIPS/eip-1459
[2] https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/
[3] http://noiseprotocol.org/noise.html
[4] https://noiseexplorer.com/patterns/NK/
[5] https://noiseexplorer.com/patterns/IK/

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Conclusions

This brief consultancy exercise, which focused on analyzing the Ethereum Node Discovery Protocol v5, concludes on a positive note. After spending five days on the scope in late 2019 and early 2020, two members of the Cure53 team can confirm that this item of the Ethereum scope makes a strong impression.

To give some details, it can be reiterated that the protocol's handshake and wire format were both formally examined and the evaluation extended to exotic XOR-based constructions as well. The latter were specifically named as focal points for this assessment by the Ethereum team. Cure53 made only minor observations about possible improvements and shortcomings that the team responsible for the security of the Discv5 protocol could consider.

A call was scheduled with the client to discuss the outcomes as regards handshake authentication, PSK support, bootstrap nodes, key compromise impersonation attacks, XOR constructions, as well as Discv5's custom wire format. The report follows up on the matters tackled on the call and elaborate on the issues through proper documentation. First, authentication-related findings can be found in ETH-06-001, which additionally offers some comments on mitigations strategies that the ETH team has already been planning. Secondly, ETH-06-002 suggests adding pre-shared key support to the Discv5 protocol as an optional measure to reinforce authentication.

At this stage, Cure53 has no further concerns to report. In light of the observations made during this late 2019-early 2020 consultancy exercise, Cure53 is happy to report that the Ethereum Node Discovery Protocol v5 may be seen as sound and robust.

Cure53 would like to thank Martin Holst Swende and Felix Lange from the Ethereum team for their excellent project coordination, support and assistance, both before and during this assignment.