30 October 2020 Study · Blockchain · Web & Cloud

IPFS Security Analysis

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2020-10-29
Source https://technology2.a-sit.at/en/publications/ipfs-security-analysis/

During this project, IPFS, a decentralized peer-to-peer hypermedia system, was subjected to a security analysis. Vulnerabilities with serious consequences could be found, which were exploitable to segment the entire IPFS main network at will and to bring it to a standstill. A corresponding attack was implemented and successfully evaluated. The fact that this incurs hardly any cost is particularly critical in this context, as it means that the attack could be carried out by anyone. Protocol Labs, the company that is driving IPFS development and that acts as this open source project's main sponsor was informed promptly. This lead led to a variety of mitigations being implemented. As part of a responsible disclosure process, this project's report was not published before the end of October 2020 and its approval was coordinated with Protocol Labs. Protocol Labs published a post on the official IPFS blog on this subject. In addition, a scientific publication (currently under review) was prepared on the project results.

Links

IPFS Blog

Paper Pre-Print