Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Cure53 Security Assessment of Obsidian Clients & UI, Management Summary, 09.2024

Cure53, Dr.-Ing. M. Heiderich, M. Pedhapati, C. Luders, Dr. D. Bleichenbacher, Dr. N. Kobeissi

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and security assessment against the Obsidian Client software, with an explicit focus on the client:

- Repository in scope: *obsidian-master/*
  - Commit ID: 220b580d4fd4ab13250703a3efd36310d1b7f0f2
- Repository in scope: *obsidian-static-master/*
  - Commit ID: fbf3d1ab4fb01047e36e0b571a5f020268137650

To provide context regarding the timeline and resource allocation for DYL-03, Cure53 was hired by Dynalist Inc. in August 2024 to perform this security assessment in September 2024, specifically in CW38, and invested a total of four days to achieve the desired coverage for this task. A team of five senior testers was formed and assigned to the preparation, execution, documentation, and delivery of this project.

It is important to note that this is not the first security-focused collaboration between Cure53 and Obsidian. The Obsidian client was previously analyzed by Cure53 in November 2023, during the project designated as DYL-01. This means that the findings from previous pentests and source code audits against the Obsidian client, which revealed several vulnerabilities, could be leveraged to inform this second iteration of examinations targeting the same scope. Due to the nature of the tasks involved in DYL-03, the assessment was structured into a single work package (WP).

- **WP1**: Crystal-box pentests & code audits against Obsidian clients & UI

In alignment with the specified WP title, a crystal-box methodology was employed for this assessment. Cure53 was furnished with access to the Obsidian GitHub repository, pertinent documentation, and all other requisite resources to ensure successful completion of the tests.

The project was successfully completed without encountering any major obstacles. To ensure a smooth transition into the testing phase, all necessary preparations were completed in CW37. A dedicated and private Discord channel was established to facilitate communication between Cure53 testers and internal staff from Obsidian. This channel provided an open forum for discussions and exchange of information.

Cure53 found that the quality of all project-related interactions was consistently high, with minimal need for clarification or additional questions. This effective communication contributed positively to the overall project results. The clear and careful preparation of the scope helped to avoid significant roadblocks. Cure53 provided regular updates on the test progress and emerging findings, but live reporting was not specifically requested for DYL-03.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

The Cure53 team achieved excellent coverage of the WP1 objectives. Of the eight security-related discoveries, six were classified as security vulnerabilities and two were categorized as general weaknesses with lower exploitation potential. Notably, one of the two general weaknesses was a False Positive issue (DYL-03-006), while the other could be considered a feature within the Obsidian client rather than a security issue.

Identified Vulnerabilities

- **DYL-03-001 WP1**: Flawed remediation of CVE-2022-36450 (Low) **FIXED**
- **DYL-03-002 WP1**: Deeplink opens arbitrary URLs and leaks filenames (Low) **FIXED**
- **DYL-03-003 WP1**: DoS caused by missing limits in window-opening (Medium) **FIXED**
- **DYL-03-004 WP1**: URL spoofing via filtered ports (Medium) **FIXED**
- **DYL-03-005 WP1**: URL spoofing via redirect to invalid protocols (Medium) **FIXED**
- **DYL-03-007 WP1**: UXSS via bookmarks accepting JavaScript URI (Critical) **FIXED**

Miscellaneous Issues

- **DYL-03-006 False Positive**: Outdated and vulnerable dependencies in Obsidian static (Info)
- **DYL-03-008 WP1**: Markdown permits file://-protocol (Info)

The test results, while not extensive, indicate mixed outcomes. The security standing of the Obsidian client component has improved since the previous audit, as evidenced by the identification of only a single rather serious vulnerability, which addresses a new browser webview feature (see DYL-03-007). Despite the positive development of resolving most findings and CVEs from the last project, Cure53 noted that, at the time of testing, CVE-2022-36450 was still exploitable.

Concluding, it needs to be highlighted that Obsidian's swift response to address the identified issues of this audit demonstrates their commitment to ensuring a good level of security for their client. By continuing to monitor for new vulnerabilities and taking proactive measures to address them, Obsidian can further strengthen the security posture of their client component.

Cure53 would like to thank Erica Xu, Steph Ango, Shida Li, and Tony Grosinger from the Dynalist Inc. team for their excellent project coordination, support and assistance, both before and during this assignment.