Fine penetration tests for fine websites

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

Cure53 Security Assessment of Obsidian Clients & UI, Management Summary, 01.2024

Cure53, Dr.-Ing. M. Heiderich, M. Pedhapati, Dr. D. Bleichenbacher, H. Li, R. Maini, H. Jaiswal, C. Luders

Cure53, a Berlin-based IT security consultancy, has completed a security assessment against the Obsidian client software complex, specifically targeting the client software itself and the exposed client software UI-related attack surface:

- Repository in scope: */obsidian*
  - Commit ID: da7a11f80520c0535afff08f09ee9e062230cb02
- Repository in scope: */obsidian-static*
  - Commit ID: d3cd2d346872e96c60fce60e73d1524af2e20c69

The Obsidian project management team submitted the request for this procedure in September 2023, and upon acceptance of the proposal, Cure53 scheduled the analysis shortly thereafter in November 2023, namely in calendar week 45 and CW46.

A total of eighteen days were invested in order to achieve the expected coverage for this particular task (labelled *DYN-01*). It should also be noted that a team of six Cure53 testers and auditors was set up and tasked with the preparation, execution and completion of this project.

For optimal structuring and tracking of tasks, the work was structured using one distinct Work Package (WP):

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

The methodology followed a crystal-box strategy, where support materials such as sources, documentation and other assorted entities were provided to facilitate the undertakings. In addition, documentation was shared to ensure that the project could be executed according to the agreed framework.

A private and shared Discord channel was set up for communication between the two organizations. In general, the discourse was seamless and highly conducive to a productive pentest.

The exhaustive scope setup meant that cross-team queries about the objectives or underlying infrastructure were minimal overall, while the process was not delayed or blocked outright at any point. The testers also provided numerous progress and status updates during the live reporting process, which served to raise awareness of certain high-profile findings at the point of discovery.

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

The Cure53 team achieved very good coverage of the scope items. Of the four security-related discoveries from WP1 mentioned above, all four were classified as security vulnerabilities and none as general weaknesses with low exploitation potential:

- **DYL-01-001 WP1**: CORS bypass via flawed URL validation (High)
- **DYL-01-006 WP1**: Arbitrary file read via local file embedding (Critical)
- **DYL-01-007 WP1**: Arbitrary file write via path traversal in Sync plugin (Critical)
- **DYL-01-009 WP1**: App protocol origin leak via CSS snippets (High)

As the final phase of this project, in late December 2023, Cure53 conducted a remediation verification phase to examine how the Obsidian scope has improved over time and in relation to the findings communicated. In this area, the audit team is pleased to report that all vulnerabilities have been properly addressed and the recommendations from the assessment have been properly followed. Cure53 was able to review the diffs created by the Obsidian team to fix the reported issues and was therefore able to make reliable judgments about the quality of the fixes.

From the perspective of the Cure53 team, appropriate steps have been taken to ensure that good fixes have been created and are now in effect for the Obsidian clients, UI and features.

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