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 Sync API, Server & Crypto, 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 Sync software, with an explicit focus on the server components and cryptographic implementations within Obsidian Sync:

- Branch: *obsidian-master*
  - Commit ID: 220b580d4fd4ab13250703a3efd36310d1b7f0f2
- Branch: *obsidian-static-master/*
  - Commit ID: fbf3d1ab4fb01047e36e0b571a5f020268137650

Dynalist Inc. requested the audit, labelled as DYL-04, in August 2024. This is the latest in a series of security-focused collaborations between Obsidian and Cure53. Previously, Cure53 conducted the audits DYL-01 (November 2023) and DYL-03 (parallel to DYL-04), both targeting the Obsidian Clients and Sync components.

Cure53 successfully concluded its research activities for audit DYL-04 in September 2024, specifically during CW38. To ensure comprehensive coverage of the audit objectives, a total of eight days were dedicated to this endeavor. A team of five seasoned security testers was assembled to undertake the meticulous preparation, execution, documentation, and delivery of this project.

Given the nature of the tasks envisioned for DYL-04, the assessment was split into two work packages (WPs):

- **WP1**: Crystal-box pentests & code audits against Obsidian Sync API & server
- **WP2**: Crystal-box pentests & cryptography reviews of Obsidian Sync crypto code

As indicated by the WP titles, the crystal-box methodology was employed for both WPs, with cryptographic reviewing methods incorporated into WP2. Cure53 was granted access to the Obsidian GitHub repository, relevant documentation, and all other necessary resources to successfully complete the tests.

The project was completed in a satisfactory manner, with no significant issues encountered. To guarantee a seamless transition into the testing phase, all essential preparations were completed in CW37. A private Discord channel was set up to ensure clear communication between the Cure53 testers and the internal Obsidian team. This channel served as an open forum for discussions and the exchange of information.

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

Cure53 determined that all project-related interactions consistently demonstrated a high level of quality, with minimal necessity for further clarification or inquiry. This effective communication had a positive impact on the overall project results. The meticulous preparation of the scope helped to circumvent any significant obstacles. Cure53 provided regular updates on the test progress and emerging findings, but there was no specific request for live reporting on DYL-04.

The Cure53 team achieved a high level of coverage for the WP1 and WP2 objectives. During their security assessment, they identified six security-related issues. Five of these were classified as security vulnerabilities, while one was deemed a general weakness with lower exploitation potential. After careful review, it was mutually agreed that the single general weakness was a False Positive finding.

Identified Vulnerabilities

- **DYL-04-001 WP1**: Password hashing not memory-hard (Low)
- **DYL-04-002 WP1**: Internal comms method relies on single hard-coded secret (Low) **FIXED**
- **DYL-04-003 WP1**: Hard-coded secrets give access to development tools (Low)
- **DYL-04-005 WP1**: Key mgmt. confusion in managed vault encryption mode (Medium) **FIXED**
- **DYL-04-006 WP1**: Vault auth reveals information about encryption key (Low) **FIXED**

Miscellaneous Issues

- **DYL-04-004 False Positive**: Ineffective string validation function (Info)

Cure53 was favorably impressed by the enhanced backend security features implemented in the latest version of the Obsidian Sync software. In comparison to its predecessors, Obsidian has made substantial progress in fortifying its cryptographic mechanisms. Despite these advancements, there remain areas that warrant further attention. The password hashing algorithms should be fortified, and the opt-in managed encryption mode should be hardened along with the recommendations made in DYL-04-005. It is, however, good to see that Obsidian already made the proposed changes to their official documentation and warn their users about the drawbacks of standard managed encryption.

It is imperative to acknowledge the swift actions taken by the Obsidian team in working on addressing several of these identified vulnerabilities shortly after the conclusion of the audit. This proactive approach underscores the Obsidian team's unwavering dedication to safeguarding the user experience.

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.