Security Consultation

ZCG

Scope

The Zcash Community Grants program (ZCG) has requested that Least Authority provide consulting services by reviewing zwallet to assess the client's vulnerability management strategy and offer recommendations for improvement.

Reviewed Resources

https://github.com/hhanh00/zwallet

https://ywallet.app

Recommendations

We reviewed the publicly accessible resources for ways researchers may report vulnerabilities to the zwallet team and could not find any contact information for a private and encrypted channel, neither on GitHub nor on the website. As some found vulnerabilities may leave wallet users at risk until a remediation can be implemented, a public GitHub issue may not always be the best form of receiving vulnerability disclosures. We recommend aiding researchers in responsibly disclosing vulnerabilities to the zwallet team, introducing internal processes to handle vulnerability disclosure and incident response, and adhering to best practices for the prevention of security incidents. Our recommendations are as follows:

Recommendation 1: Add a Communication Channel

- During the review, we could not find any contact information for a private and encrypted channel for researchers to disclose vulnerabilities on zwallet's GitHub or the zwallet website. We recommend that the zwallet project have an easily accessible, dedicated form of communication to allow security researchers to securely and confidently contact the zwallet team in case any vulnerabilities are identified. This could be, for example, a dedicated email address, a Signal username, or a webform. The chosen form of communication should provide transport security (e.g., Signal messaging, https, or encrypted email).

Recommendation 2: Add a Vulnerability Disclosure Policy

- Additionally, we could not find a vulnerability disclosure policy on zwallet's GitHub (or `security.md`) or the zwallet website. We recommend that a vulnerability disclosure policy be made publicly accessible (see [1] for a template of such a policy). The policy should provide detail on scope (covered list of products and endpoints), the form of reporting, and other details important in the vulnerability disclosure process, including but not limited to:
  - Expected form of communication for vulnerability disclosure (see Recommendation 1);
  - Request for non-disclosure to third parties;
  - Legal authorization for security research;

  - Expected timeline of the process along with its description (this may include sharing the status of a reported vulnerability or its remediation with the reporter);
  - Existence or absence of a bug bounty program, along with its conditions; and
  - Description of the expected form of the report (impact, steps for reproducing the issue or proof-of-concept exploit, and root cause analysis, if possible).
- We also recommend that the zwallet team consult their legal team to ensure compliance with the applicable law.

Recommendation 3: Create an Internal Process for Handling Vulnerability Reports

- Our team did not find publicly available information on zwallet's internal handling of reported vulnerabilities. We recommend that the zwallet team establish an internal process for dealing with reported vulnerabilities. This process should cover the following:
  - Assigning responsible team members for communicating with researchers and initiating the internal process to remediation;
  - Acknowledging the report in a response and communicating about further processes and expected timelines to the researcher;
  - Adding the reported vulnerability to any internal bug-tracking or ticketing system in order to establish documentation of each step;
  - Triaging steps, which include impact analysis, reproducing and confirming issues, as well as the prioritization and communication of confirmation to the researcher;
  - Planning remediation according to prioritization;
  - Planning any needed outside communication to affected third parties (users, other projects, etc.); and
  - Performing the verification of the remediation or mitigation with the researcher.

Recommendation 4: Create a Process for Incident Response

- We did not find publicly available information on zwallet's incident response handling. We recommend that the zwallet team introduce an internal process for handling security incidents, including but not limited to supply-chain attacks, malware campaigns that may target zwallet products, infection or other attacks on zwallet's development or production systems, and data breaches. Example checklists from government bodies can be found in [2], [3], and [4]. This internal process could require:
  - Specifying whether incidents (and what kind of incidents, more specifically) should be handled internally or by an external party;
  - Reporting security incidents to users and related projects and companies;
  - Introducing a triage process — similar to what is mentioned in Recommendation 3 (incident confirmation, impact and urgency review, and root cause analysis); and
  - Reporting any security incidents in the country zwallet operates in, if required by law.

Recommendation 5: Add Safeguards for Preventing Incidents

- Although we did not review any measures in regards to testing, dependency handling, and continuous integration, our team noted that following steps can help prevent incidents and unpatched vulnerabilities in release versions:
  - A wide range of testing (e.g., adding integration testing, testing edge-cases and properties (fuzzing and property-based testing), and adding integrated testing in CI;
  - Adhering to best practices in code review in the development process (utilizing GitHub pull requests and requiring code reviews before merging);
  - Reviewing and updating dependencies, as well as integrating dependency checks and static analysis in CI, wherever possible;
  - Keeping up with any security news within the ecosystem and any other utilized platforms to detect potential threats early; and

- Reviewing the internal operational security, including, for example, internal best practices on handling secrets, security of development devices and infrastructure, as well as the storage and security of user data.

Resources

[1] https://www.cisa.gov/vulnerability-disclosure-policy-template
[2] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=916838&cms_pos=2
[3] https://www.cisa.gov/resources-tools/resources/cyber-incident-guide
[4] https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-response-checklist

Consulting Team

Anna Kaplan, Cryptography Researcher and Engineer

Anna is a mathematician and cryptographer, with experience working at Zcash Foundation and IBM Research. Besides being interested in new cryptographic advancements, she is also very passionate about communicating all things cryptography and privacy.

AC, Security Researcher

Ann-Christine holds an MSc in Computer Science and is a former research assistant at the Hamburg University of Technology. She is passionate about learning and understanding new technologies, languages, types of vulnerabilities, and attack vectors. Her work focuses on software and application security, as she believes secure and privacy-focused software and technologies should be a fundamental human right for all.

About Least Authority

We believe that people have a fundamental right to privacy and that the use of secure solutions enables people to more freely use the Internet and other connected technologies. We provide security consulting services to help others make their solutions more resistant to unauthorized access to data and unintended manipulation of the system. We support teams from the design phase through the production launch and after.

The Least Authority team has skills for reviewing code in multiple Languages, such as C, C++, Python, Haskell, Rust, Node.js, Solidity, Go, JavaScript, ZoKrates, and circom, for common security vulnerabilities and specific attack vectors. The team has reviewed implementations of cryptographic protocols and distributed system architecture in cryptocurrency, blockchains, payments, smart contracts, zero-knowledge protocols, and consensus protocols. Additionally, the team can utilize various tools to scan code and networks and build custom tools as necessary.

Least Authority was formed in 2011 to create and further empower freedom-compatible technologies. We moved the company to Berlin in 2016 and continue to expand our efforts. We are an international team that believes we can have a significant impact on the world by being transparent and open about the work we do.

For more information about our security consulting, please visit https://leastauthority.com/security-consulting.