Zel Community Bug Bounty Program

Realizing that we are stronger when we are together as a team, the Zel Community maintains a robust Bug Bounty Program to reward security researchers who invest their time and effort through the responsible disclosure of qualifying security vulnerabilities.

Responsible Disclosure Policy

To encourage responsible disclosure, we promise we won’t take any legal action against you if you give us reasonable time to investigate and mitigate an issue before disclosing the vulnerability publicly.

Rule of Engagements

- Adhere to the Responsible Disclosure Policy
- Make a good faith effort to not interrupt or degrade our service
- Do not attempt to gain unauthorized access to user’s account, assets or information (use your own test account)
- Do not modify any files or data, including permissions, and do not intentionally view or access any data beyond what is needed to prove the vulnerability
- Do not exploit a security issue you discover for any reason
- We publish a list of researchers who have submitted valid security reports
- We reserve the right to publish reports (and accompanying updates) pertaining to this case

Eligibility Requirements

We have the right to remove you from the Bug Bounty Program and disqualify you from receiving any bounty rewards if you:

- Are in violation of any national, state, or local law or regulation
- Engage as a malicious person (evidently committed in cybercrime; such as but not limited to: scams, spams, extorts/ransoms, defacement, hacktivist, etc)

Service in Scope

- (Apps): ZelCore (Win/Linux/MacOS X) - must be on the latest/recent update (released in less than 30 days)
- (Mobile): ZelCore Mobile - latest available release on Google Play store and Apple App store
- (Libraries): zeltrezjs library
- (Website): zel.network, zelcore.io, zel.id, my.zel.cash
- (Email): @zel.network, @zel.cash
- (Open Source): Zel/Zelnode Daemon, Flux, Zel-ID, etc.
- (Infra): ZelCore Explorers or Rates servers hosted by Zel Team

Out-of-scope Service

- Third-party libraries
- Infrastructure not managed by Zel Teams such as Public Explorers and ZelNodes run community members

Qualifying Bugs

- Injection flaws such as SQL, noQSL, OS injection that tricked command interpreter into executing unintended commands without proper authorization.
- Broken authentication/session management that allows compromise of passwords, keys, or session tokens
- Sensitive data exposure due to improper protection of data via insecure API or flaw in cryptography implementation3
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF) for sensitive functions in a privileged context
- Server-side or remote code execution (RCE)
- Insecure Direct Object References
- Privilege Escalation
- Significant Security Misconfiguration (when not caused by user)
- Directory Traversal
- Open Redirects
- Spoofing enablement
- Any significant abuse-related methodologies that could lead to significant harm

Non-Qualifying Bugs

- Non-original or previously disclosed/reported bugs (which fixes currently underway).
- Any attempts of non-technical attacks such as social engineering, phishing, or physical attacks against our entities or infrastructure.
- Any attempts of degrading/damaging the reliability or integrity of our services (such as DDoS attacks, blackhat SEO techniques, spamming, or similar questionable acts)
- software/module/packages not directly produced by Zel Development Team
- Domains hosted by third parties (e.g.: Github, Gitlab, etc)
- Subdomains operated by third parties (e.g: info.zel.cash)
- Any Zel branded services operated by third parties

How to Report a Security Vulnerability

Send an email with your bug report detail to **whitehats@zel.network**
Only email submission will be considered valid. Any other submission channel will not be entertained.

Our Promise

We will do our best to respond to your submission as quickly as possible, keep you updated on the fix, and award bounty rewards where appropriate in $ZEL cryptocurrency only. WE are thankful for your contribution and all the efforts to make the Zel project a success.