Zivver - Vulnerability Disclosure Policy

Version: 1.0

Date: May 11, 2023

Zivver looks forward to working with the security community to find vulnerabilities in order to keep our businesses and customers safe. Please read our policy carefully before submitting a report.

1.1 - Response Targets

Zivver will make its best effort to meet the following SLAs for hackers participating in our program:

Type of Response	SLA in business days
First Response	5 days
Time to Triage	10 days
Time to Resolution	depends on severity and complexity

We'll try to keep you informed about our progress throughout the process.

1.2 - Disclosure Policy

As this is a private program, please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the organization.

zivver

1.3 - Program Rules

- Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue may not be marked as triaged.
- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only triage the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be treated as one valid report.
- Social engineering (e.g. phishing, vishing, smishing) is prohibited.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.

1.4 - Product scopes

The following products are considered in/out of scope

In-scope

Product	Description	Impact
Domain	**app.zivver.com** This is the main Zivver web application.To begin testing, please register on app.zivver.com with your personal email address. Our documentation is available at docs.zivver.com. You can learn more there about how the service works and how the clients (web, mobile and plugins) can be used.	Critical
Domain	**collector.zivver.com**	Critical
Domain	**downloads.zivver.com** Zivver Office plugin downloads, sourced from an Amazon S3 bucket.	High

Domain	**docs.zivver.com**	Low
Domain	**img.zivver.com**	Low
Android: Play Store	**com.zivver.app**	Critical
iOS: App Store	**com.zivver.app**	Critical

Out of Scope

Any report made on out-of scope domains are automatically closed

Product	Description
Domain	**support.zivver.com**
Domain	**zivver.eu**
Domain	**survey.zivver.com**
Domain	**workat.zivver.eu** This asset is from a 3rd party called Recruitee. Feel free to submit your report at their program https://recruitee.com/vulnerability
Domain	**get.zivver.eu** 3rd party marketing landing pages service. We control this domain through Unbounce, and it is not vulnerable to subdomain takeovers, despite the frontpage not returning content.

Domain	**get.zivver.com** 3rd party marketing landing pages service. We control this domain through Unbounce, and it is not vulnerable to subdomain takeovers, despite the frontpage not returning content.

1.5 - Out-of-scope vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario/exploitability, and (2) security impact of the bug. The following issues are considered out of scope:

⚠️ **Popular duplicate topics:**

- **MULTIFACTOR AUTHENTICATION (MFA) 'BYPASS'** on the web application (client-side): MFA is intended to be an optional feature, rather than a hard requirement, for Zivver users. While the app may presently appear to enforce a hard requirement for MFA in places, that is not a strategic intent and the design will be re-evaluated in upcoming releases. Please do not report client-side MFA bypass vulnerabilities here.
- **Reflected (Self) XSS, HTML**: Unless a clear security impact can be demonstrated (does not require unlikely user interaction and concerns a domain where sensitive user information is stored), we are not interested in receiving reports on reflected (self) XSS or HTML injection issues.

Also out of scope:

- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)

- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction.
- Not enforcing certificate pinning.

1.6 - Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If a third party against you initiates legal action in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Thank you for helping keep Zivver and our users safe!