Interpres Security

Vulnerability Disclosure Program

Interpres is committed to protecting the privacy and security of our customers. Although we have taken every effort to minimize all the security bugs in our systems, we realize that something may have been missed. We encourage individual security researchers to study/analyze our platform to make it even safer. Our Vulnerability Disclosure Program (VDP) is intended to minimize any security flaws found in our infrastructure and software. If you believe you have found a security vulnerability in our platform, please contact us as soon as possible. We will investigate all legitimate reports and do our best to address the issue quickly. Before reporting the issue, please take a moment to review this page, which includes our disclosure policy, guidelines, rules, the program's scope, rewards, and how to contact us.

Responsible Disclosure Policy

- You give us a reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
- You make a reasonable faith effort to avoid privacy violations and disruptions to others, including (but not limited to) unauthorized access to or destruction of data and interruption or degradation of our services.
- You do not exploit a security issue you discover for any reason. (This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for further problems.)
- You do not intentionally violate any other applicable laws or regulations, including (but not limited to) laws and regulations prohibiting unauthorized access to data.
- For this policy, you are not authorized to access user data or company data, including (but not limited to) personally identifiable information and data relating to an identified or identifiable natural person.

Guidelines & Rules

Participating in Interpres' VDP requires you to follow our guidelines. The following guidelines are required to be eligible for rewards under this disclosure program:

Residents in U.S. sanctioned countries (Cuba, Iran, Sudan, Syria, and North Korea) are ineligible.

- Don't violate the privacy of other users, destroy data, disrupt our services, etc.
- Don't request updates on an hourly basis. We are handling dozens of reporters daily, and spam impacts JumpCloud's efficiency.
- Only target your accounts in the process of investigating any bugs/findings. Don't focus, attempt to access, or otherwise disrupt the accounts of other users.

- Don’t target our physical security measures or attempt to use social engineering, spam, or distributed denial of service (DDOS) attacks.
- If you find a severe vulnerability that allows system access, you must not proceed further.
- Interpres decides to determine when and how bugs should be addressed and fixed.
- Disclosing bugs to a party other than Interpres is forbidden; all bug reports are to remain at the reporter and Interpres discretion.
- Threatening behavior of any kind will automatically disqualify you from participating in the program.
- Exploiting or misusing the vulnerability for own or other’s benefit will automatically disqualify the report.
- Bug disclosure communications with Interpres Security team are to remain confidential. Researchers must destroy all artifacts created to document vulnerabilities (POC code, videos, screenshots) after the bug report is closed.

Vulnerability Disclosure Program Scope

The following services and domains are considered in scope:

In-Scope Endpoints and Systems

These specific endpoints and our endpoints are considered in scope:

- Interpres core API service (api.interpres.io)
- Interpres Auth Service (auth.interpres.io)
- Interpres Auth user and admin Auth (auth.interpres.io)
- Interpres Identity provider service (idp.interpres.io)
- Interpres User Interface (interpres.io)
- Interpres App Integrations API endpoint app.interpres.io)
- Interpres streaming event offloader service (kafka offloader data.interpres.io)
- interpres Service Provider endpoint for SAML (sso.interpres.io)

Out of Scope Endpoints and Systems

- Interpres Support Site (support.interpressecurity.com)
- Interpres Main Site (interpressecurity.com)
- Interpres Docs Site (docs.interpressecurity.com)
- Vulnerabilities on sites hosted by third parties unless they lead to a weakness on any scoped endpoint.

In-Scope Vulnerabilities

Generally speaking, any bug that poses a significant vulnerability could be eligible for a reward. It is entirely at Interpres' discretion to decide whether a bug is significant enough to qualify for an award. Security issues that typically would be eligible (though not necessarily in all cases) include:

- Cross-Site Request Forgery (CSRF)
- Cross-Site Scripting (XSS)
- Code Executions
- SQL injections
- Server-Side Request Forgery (SSRF)
- Privilege Escalations
- Authentication Bypasses
- File inclusions (Local & Remote)
- Protection Mechanism bypasses (CSRF bypass, etc.)
- Leakage of sensitive data
- Directory Traversal
- Administration portals without an authentication mechanism
- Open redirects which allow stealing tokens/secrets
- Remote Code Execution / Arbitrary Code Execution

Out of Scope Vulnerabilities

Things that are not eligible for reward include:

- Social Engineering
- Lack of rate-limiting mechanisms
- Open redirects without a severe impact
- Application stack traces (path disclosures, etc.)
- Self-type Cross-Site Scripting / Self-XSS
- Vulnerabilities that require Man in the Middle (MiTM) attacks
- Denial of Service attacks
- CSRF issues on actions with minimal impact
- Cache Poisoning
- Clickjacking
- Incomplete or missing SPF/DMARC/DKIM records
- HSTS not enabled on *.interpressecurity.com websites
- Brute force attacks
- Security practices (banner revealing a software version, missing security headers, etc.)
- Bugs that do not have security implications
- Vulnerabilities on sites hosted by third parties unless they lead to a weakness on the main website

- Vulnerabilities are contingent on physical attack, social engineering, spamming, DDOS attack, etc.
- Vulnerabilities affecting outdated or unpatched browsers/operating systems
- Bugs already are known to us, or previously reported by someone else (reward goes to the first reporter)
- Issues that aren't reproducible

Reporting

Send an email to vuln_report@interpressecurity.com using the PGP key located here, with information about the vulnerability and detailed steps on how to replicate it.

- The report must pertain to an item explicitly listed under our in-scope vulnerabilities section.
- The report should also contain as much information as you can–ideally, a description of your findings, the steps needed to reproduce it, and the vulnerable component.
- If you need to share screenshots/videos, please upload it to Google Drive (or any other upload service) and share with us the links to those files.

We will make every effort to respond to accurate reports within seven business days.

Interpres will utilize Bugcrowd's VRT for initial prioritization and review its overall impact for further prioritization based upon interrpes Vulnerability Management Program.

All Assessments are considered final.