Vulnerability Disclosure Policy for AlertGPS

AlertGPS is committed to enhancing the safety and operational efficiency of mobile and lone workers through advanced technology solutions. This policy underscores our dedication to security and reflects our values and legal obligations to security researchers providing valuable insights.

Initial Scope

The Vulnerability Disclosure Program at AlertGPS currently includes:

- **AlertGPS Service**: Our web platform enhances safety and operational efficiency for mobile workers.
- **ActiveHalo+® Device**: A 4G LTE safety wearable paired with an enterprise cloud-based IoT platform, offering location services, two-way SOS voice calls, fall detection, and real-time support.

We invite security vulnerability reports solely for the listed products and services.

Third-Party Bugs

AlertGPS reserves the right to forward details of issues reported to it if they affect third-party components or external projects. Throughout this process, our team will continue to coordinate and communicate with researchers.

Legal Posture

AlertGPS commits to not initiating legal action against individuals who submit vulnerability reports through our designated channels. We welcome reports on the specified products, provided that individuals:

- Comply with all applicable laws and conduct non-harmful testing, ensuring no disruption to the organization's services or systems.
- Obtain explicit consent from affected customers before engaging in testing on their devices or software, avoiding unnecessary, excessive, or significant data access.
- Refrain from employing social engineering tactics on employees or contractors of the organization.
- Maintain the integrity and operational efficiency of services by not interrupting or degrading user experience.
- Delay any public disclosure of vulnerabilities until after a mutually agreed-upon timeframe has been established and adhered to.

How to Submit a Vulnerability

Please email vulnerability reports to AlertGPS's Product Security Team at: security@alertgps.com.

Preference, Prioritization, and Acceptance Criteria

Submissions are prioritized based on:

- Report quality and completeness.
- Inclusion of proof-of-concept code.
- Relevance to the listed products and services.

Expectations for submitters:

- A response within 5 business days.
- Transparency regarding remediation timelines.
- Open communication throughout the review process.
- Acknowledgment upon fixing the validated vulnerabilities.
- In cases of communication breakdowns or challenges, AlertGPS may involve a neutral third party to facilitate resolution.

Version History

Version 1.0 (2-April-2024): Initial release of the policy.