SONOFF’s vulnerability disclosure policy

SONOFF recognizes the importance of the security community in keeping our products, offerings, services, and websites safe for our customers and users. We are grateful for the contribution to our vulnerability disclosure work from any well-intentioned, ethical security researchers. All the vulnerability reports will be handled by SONOFF Security Team. This team will coordinate with other SONOFF teams to investigate, and if needed, identify the appropriate response plan. Maintaining communication between all involved parties, both internal and external, is a key component of our vulnerability response process.

Scope

- Any vulnerability disclosure attempt is limited to exploitable security vulnerabilities and CVE found in SONOFF products, offerings, services, and websites that are still being supported by SONOFF. Check our software lifecycle to determine which product version is still supported.

Guidance

This policy prohibits the performance of the following activities:

- Violate any applicable local or global law in the process of vulnerability disclosure
- Access, use, alter or compromise in any manner any SONOFF data;
- Conduct any act that may adversely affect the operation of SONOFF products, software, offerings, websites, or services;
- Attempt to access, disrupt, or compromise any data that is not your own, or further exploit a confirmed vulnerability;
- Cause harm to SONOFF or our customers;
- Include any information that may identify an individual (such as a name, contact information, IP address, or other similar information) in vulnerability reports;
- Do not publicly disclose or share the vulnerability or methods to exploit with any third party without the consent of SONOFF team.

SONOFF reserves the legal right to appeal to law with regards to any inappropriate activities which may cause any damage to or cast a negative impact on SONOFF or SONOFF’s business reputation in the process of vulnerability disclosure.

It is at SONOFF’s sole discretion to update or modify this policy at any time.

Any vulnerability reports submitted thereafter shall conform to the latest policy.