Vulnerability Disclosure Policy

How to Report a Vulnerability

Report suspected vulnerabilities

Security researchers, industry organizations, customers and suppliers are encouraged to work with us and report security vulnerabilities related to Yodo products and services.

Vulnerability reporting email

If you encounter or discover security issues in Yodo products and services, please report them to us by sending an email to qiuweijian@yodosmart.com.

Reporting email	Note
qiuweijian@yodosmart.com	Email subject line: Vulnerability name (for example, XXX product's XXX vulnerability)

The body text of the email can follow the format below, or you can choose the necessary information to send.

1) Name of the reporting individual or organization, and contact information
2) Vulnerability descriptions (vulnerability type and its threat)
3) Affected products and their versions
4) Technical details of potential vulnerabilities, proof of exploitation, and proof of concept (POC)
5) Suggestions for enhancing and fixing security
6) Possible vulnerability disclosure plan

Vulnerability Response

We values the vulnerability management of its products and services, supports responsible vulnerability disclosure and handling processes, and respects the research output of every security researcher. We will assign dedicated personnel to follow, analyze and handle each security issue that is reported to ensure that there is a timely resolution and response. We will send an email with the initial feedback within five working days. We will continue to follow up and provide updates on the vulnerability resolution progress until the fix is completed.
* Note: The actual time of response to the vulnerability may vary depending on its risk level and complexity.

Vulnerability awareness: Take the initiative to monitor and receive the potential security vulnerabilities and issues that are reported, and remain in contact with the vulnerability reporters.

Vulnerability verification: Verify whether potential security vulnerabilities and problems affect the security of our products, assess risks, and inform users about the rectification timeline and vulnerability levels.

Fixing vulnerabilities: Develop plans for mitigating the risks of and fixing vulnerabilities, verify the results of the vulnerability fix, and provide product upgrade packages or patches.

Vulnerability disclosure: Disclose vulnerability information when workarounds and patches are available (or when new releases are launched).

Problem improvement: After the vulnerability is disclosed, we will monitor the effectiveness of the remedy, collect customer feedback and suggestions, and update the patch/upgrade the package if necessary. Shokz will also keep improving product development and vulnerability handling processes.

Throughout the vulnerability handling process, we will strictly control the scope of the vulnerability information and limit its dissemination to only the relevant personnel involved in the vulnerability remediation. We also request that the vulnerability reporter promise to keep the vulnerability information confidential until a complete resolution is provided to the users.

We will take the necessary and reasonable measures to protect the vulnerability data that we obtain based on legal compliance. We will not voluntarily share or disclose the above data to other parties unless expressly requested to by the affected customer or if required by law.

Product Security Support Policy

We try to provide constant security updates for our IoT products. Security updates usually include the latest security patches, security vulnerability repairs, and other security improvements. We will maintain security updates for some device models for at least 10 years from the date of release.

*The corresponding security support period for the product will not be shortened on this basis. We will announce the new support period if it is extended.

List of products supporting security updates:

Type	Support period
ZD42C1	2026.7.15-2027.7.15
ZD444	2026.7.15-2027.7.15