Australia Cyber Security

Incident Response

We attach great importance to security issues and welcome all security researchers to report potential security vulnerabilities to us to improve the security of our products and services.

Vulnerability Response and Disclosure Process

Monitor and assign received vulnerabilities in a timely manner
Verify the vulnerability and confirm the exploitability and impact
Provide effective fix solutions or risk remediations measures
Investigate and confirm the complete scope of affected products
Review and publish the security advisory for the security vulnerability
Report Vulnerabilities

You can report vulnerabilities via telephone through our customer service department, or via email. The following are the detailed reporting methods:

Email: psirt@fudazn.com

Phone number: 86 574 62500010

Attention

Although we encourage investigation of potential security breaches, we cannot tolerate any activity that may interfere with legitimate users or may violate applicable computer abuse, cyber security and data protection regulations. Therefore, the following activities are prohibited:

- Modification or destruction of data

- Service disruption or degradation, such as DoS

- Disclosure of personal, proprietary or financial information

Response Time

After receiving the vulnerability you reported, we will send you vulnerability response related information within 48 hours based on the platform you used to report the vulnerability, as follows:

For vulnerabilities reported via email, we will send you a vulnerability response notice, information confirmation and feedback related to the vulnerability via email. The progress of

the vulnerability's solution development will also be continuously updated through email as soon as possible.
For vulnerabilities reported via the phone, we will send you a vulnerability response notice, information confirmation and feedback related to the vulnerability via email (gathered during the phone call). The progress of the vulnerability's solution development will also be continuously updated through email as soon as possible.
We will provide you with an update on the vulnerability within 15 business days.
* Note: Actual vulnerability response time may vary depending on the risk level and complexity of the vulnerability.

Product Support Policy Overview

We do our best to provide continuous security updates for our IoT products. The security updates generally include the latest security patches, security vulnerability fixes, and other security improvements. We will maintain the security updates for at least 10 years from the launch day of certain device models. The updates are available directly through the TUYA Smart App and can be downloaded at any time through the device settings under: “Device Update” or through pop-up messages.

*Security updates cover product hardware (firmware), pre-installed software, software that implements necessary product functions, and external control software.

Contact us

If you have any questions about our company's privacy notice, the data we hold about you, or if you wish to exercise any of your data protection rights, please do not hesitate to contact our Privacy Officer: 86 574 62500010

By visiting this page on our website: www.fudazn.com

By sending us an e-mail: psirt@fudazn.com

How to contact the competent authority
If you wish to report a complaint or if you feel that your concern has not been satisfactorily addressed by our company, you may contact the Commission of local information access

Call the Australian Cyber Security Hotline: 1300 CYBER1 (1300 292 371)
Write to the ASD's ACSC by post:
ACSC
General enquiries
PO Box 5076
KINGSTON ACT 2604
AUSTRALIA