

Report Vulnerabilities

Security Breach Response

IPEVO attaches great importance to security issues, and we welcome security researchers to provide us with feedback on potential security issues to improve the security of our products and services.

Vulnerability Response and Disclosure Process

1. Recipient

Monitor and assign received vulnerabilities in a timely manner.

2. Verification

Conduct technical verification of the effectiveness of vulnerabilities, confirming their exploitability and potential impact.

3. Solution Development

Provide effective fix solutions or risk remediations measures.

4. Affected Scope Confirmation

Investigate and confirm the complete scope of affected products.

5. Disclosure of Vulnerabilities

Review and publish security recommendations for the vulnerability after confirming the completion of all vulnerability response processes.

Vulnerability Submission

You can report vulnerabilities through via email. The following are the detailed reporting methods:

Mailbox

service@ipevo.com

The email should include at least the following information:

- Your organization and contact information
- Products and versions affected

- Description of the potential vulnerability
- Information about known exploits
- Disclosure plans
- Additional information, if any

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

Upon receipt of the vulnerability you have submitted, we will send you a notification via email within 48 hours to commence the vulnerability response, along with confirmation and feedback on the nature of the vulnerability. The subsequent progress of the vulnerability will also be continuously updated in the email as soon as possible.

* Note: Actual vulnerability response time may vary depending on the risk level and complexity of the vulnerability.

Vulnerability Disclosure Instructions

When an external party discovers or is concerned about a potential vulnerability, but we have not yet fully confirmed it, we will disclose basic information about the vulnerability and our investigation via email.

The vulnerability information shall be kept confidential until IPEVO releases

the formal security advisory to the public.

When the vulnerability has been confirmed to be fixed, new firmware will be released, and a firmware update change log will be published, containing a description of the vulnerabilities that have been solved. IPEVO HELP Center

Product Support Policy

We strive to provide continuous security updates for our products. The security updates generally include the latest patches, vulnerability fixes, and other security improvements. We will generally maintain security updates for at least six years from the launch date of a product. However, the security update situation may vary by product, so please pay attention to our announcements.

Product Type	Product Model	Release Date
DC	P2V Ultra	May 2024
DC	MP-8M	November 2022
DC	VZ-X	November 2018
DC	VZ-X Ultra	July 2024
DC	VZ-R	August 2018
DC	VZ-R Ultra	July 2024
DC	V4K	January 2018
DC	V4K Ultra	July 2024
DC	V4K PRO 120	August 2023
DC	DO-CAM	May 2020

* Note: Security update policies and products are subject to change and will be reviewed on a regular basis.