CMU3 Series Model Revision Details

1. Revision History

Model	Firmware Version	Revision Details	Date
CMU3	R1.0.0.0	1. Initial Release	2026/09/15
CMU3-R	R1.0.0.0	1. Initial Release	2026/09/15
CMU3G	R1.0.0.0	1. Initial Release	2026/09/15
CMU3G-R	R1.0.0.0	1. Initial Release	2026/09/15

2. Frequently Asked Questions (FAQ)

Q1: How long is the support period for product security updates?

A: Technical support is provided for up to **five years** from the final production date of the product (or longer if required by law). Once a product reaches its End-of-Life (EOL), firmware updates, including security patches, will no longer be provided.

Q2: How is the firmware upgraded?

A: Firmware updates for the CMU3 can be performed via two methods: local USB installation or network update. For detailed instructions, please refer to the user manual.

CMU3 Privacy Notice

MEAN WELL Enterprises Co., Ltd. respects and prioritizes user privacy and data security. This Privacy Notice outlines how data is handled for the CMU3 Controller.

1. Data Collection and Storage

All system configuration settings, monitoring data, and system logs generated during the operation of the CMU3 are stored locally on the device. MEAN WELL does not proactively collect or upload any of the aforementioned data to cloud servers.

2. Network Connectivity and Software Updates

The CMU3 supports Over-the-Air (OTA) software updates. During the update process, the device may exchange necessary connection and software version information with the update server to complete the operation.

3. Data Security

Users are responsible for properly managing device access permissions and network security settings. MEAN WELL is committed to providing security updates and necessary system maintenance to mitigate potential cybersecurity risks.

4. Revisions to This Notice

MEAN WELL reserves the right to modify or update this Privacy Notice in accordance with product functionality and regulatory requirements. The latest version will be published on our official website.

Vulnerability Disclosure Policy Announcement

MEAN WELL attaches great importance to product security. To protect **user rights and interests**, we have established a "Product Vulnerability Disclosure Policy" to ensure that security issues are **addressed promptly** and **effectively.**
If you discover a security vulnerability in our products, please follow t**he guidelines below to report it to us:**

Vulnerability Reporting Method

- Please send an email to security@meanwell.com containing detailed information about the vulnerability, including step-by-step reproduction instructions, potential impact scope, and any other relevant documentation.
- We will acknowledge receipt of your report **within 72 business hours** and maintain continuous communication regarding remediation progress and proposed solutions.

Responsible Disclosure Guidelines

- MEAN WELL is committed to handling all vulnerability disclosures responsibly, keeping all reported information strictly confidential, and responding in a timely manner.
- We kindly request security researchers or reporters to refrain from publicly disclosing related information or engaging in any form of improper exploitation before a patch or fix is completed.

Remediation Timeline

- We are committed to responding to and resolving vulnerability issues rapidly. The handling period for vulnerability disclosures is 180 days, during which we will complete evaluation, remediation, and verification.

Thank you for your cooperation in helping us maintain the security and integrity of our products. Your valuable feedback and collaboration are vital to protecting user safety and continuously optimizing our products.

For any questions or further information, please visit our official website or contact us at info@meanwell.com.

Release Date: September 15, 2026