Coordinated Vulnerability Disclosure Policy

Coordinated Vulnerability Disclosure Statement

Purmo Group (UK) Ltd is committed to ensuring the safety and security of our products and services. Purmo Group (UK) Ltd develops and deploys advanced best practice security and privacy features for our products and services. Purmo Group (UK) Ltd operates under a global coordinated vulnerability disclosure policy, which guides our incident management and all risk assessment activities relating to potential security and privacy vulnerabilities identified in our products and services. Purmo Group (UK) Ltd supports coordinated vulnerability disclosure and encourages vulnerability testing by security researchers and by customers, with responsible reporting to Purmo Group (UK) Ltd.

Coordinated Vulnerability Disclosure Process

When submitting reports of vulnerability findings, please ensure the following procedures are followed, for safe and efficient support.

Reporting Procedure:

Please email submissions to us at technical.uk@purmogroup.com

Please include in the e-mail subject the acronym: 'CVD' and provide us with your reference/advisory number and sufficient contact information, such as your organisation and contact name so that we can get in touch with you.

Providing a technical description of the concern or vulnerability:

a) Please provide information on which specific product you tested, the brand, including product name and version number; the technical infrastructure tested, including operating system and version; and any relevant additional information, such as network configuration details.
b) For web-based services, please provide the date and time of testing, URLs, the browser type and version, as well as the input provided to the application.

To help us to verify the issue, please provide any additional information, including details on the tools used to conduct the testing and any relevant test configurations. If you wrote specific proof-of-concept or exploit code, please provide a copy. Please ensure all submitted code is clearly marked as such.

If you have identified specific threats related to the vulnerability, assessed the risk, or have seen the vulnerability being exploited, please provide that information.

When possible, provide the report in English to expedite the process.

Product Security Vulnerability Report Assessment and Action:

1. Purmo Group (UK) Ltd will acknowledge receiving your report within two business days.
2. Purmo Group (UK) Ltd will provide you with a unique tracking number for your report.

3. Purmo Group (UK) Ltd will assign a contact person to each case.
4. Purmo Group (UK) Ltd will investigate the report.
5. Purmo Group (UK) Ltd will keep you informed on the status of your report.
6. If the vulnerability is actually in a 3rd party component which is part of our product/service, we will refer the report to that 3rd party and advise you of that notification. To that end, please inform us whether it is permissible in such cases to provide your contact information to the 3rd party.
7. Upon receiving a vulnerability report, Purmo Group (UK) Ltd will:
   a) Verify the reported vulnerability.
   b) Asses the risk level of the reported vulnerability.
   c) Work on a resolution.
   d) Perform QA/validation testing on the resolution.
   e) Release the resolution.
   f) Share lessons learned with development teams.
8. Purmo Group (UK) Ltd will use existing customer notification processes to manage the release of patches or security fixes, which may include direct customer notification or public release of an advisory notification on our website.

Vulnerability Risk Classification

Negligible Risk	1. Bug problems unrelated to security, including but not limited to slow opening of web pages and disordered styles. 2. The report submitted is too simple to be reproduced according to the report content, including but not limited to the vulnerabilities that cannot be reproduced through repeated communication with the vulnerability reviewer. 3. Products, APPs or modules not under maintenance Vulnerabilities of general protocols such as WIFI, MQTT, BLE, and Zigbee
Low Risk	1. Vulnerabilities that can be exploited for phishing attacks, including but not limited to URL redirection vulnerabilities. 2. Logic design defects of the system. 3. Minor information disclosure vulnerabilities, including but not limited to path disclosure, .git file disclosure, and business log content of the service side.
Medium Risk	1. General information disclosure, including but not limited to plaintext storage password of mobile client end, download of source code compressed package containing sensitive information of server or database, etc. 2. Logic design defects of the system, such as bypassing commodity postage, payment vulnerabilities, etc.
High Risk	1. Vulnerabilities directly leading to the disclosure of sensitive information of the online server, including but not limited to disclosure of source code of the core system, disclosure of information related to user account payment or the downloading of sensitive log files of the server. 2. Vulnerabilities that affect the normal operation of online services, such as denial of service of the application layer. 3. Logical design defects in the system, which can lead to unauthorised operation, such as unauthorised access to sensitive information.

Critical Risk	1. Vulnerabilities of remote direct access to system permissions (server permissions, client permissions, intelligent devices), including but not limited to arbitrary code execution, arbitrary command execution, and uploading and adoption of Trojan horses. 2. Mobile terminal: vulnerabilities of remote code execution. 3. Device terminal: vulnerabilities causing a permanent denial of service on the device, including but not limited to permanent denial of service attack (the device can no longer be used: it is completely permanently damaged, or the entire system needs to be rewritten) initiated remotely by the system device, that physical contact with the device is not allowed during an attack, and that the attack needs to be replicated in batches quickly

Notice:

In case you decide to share any information with Purmo Group (UK) Ltd, you agree that the information you submit will be considered as non-proprietary and non-confidential and that Purmo Group (UK) Ltd is allowed to use such information in any manner, in whole or in part, without any restriction. Furthermore, you agree that submitting information does not create any rights for you or any obligation for Purmo Group (UK) Ltd.

Last update: 16/01/2026