**Vulnerability Reporting Template v1.0**

**Thank you for reporting any suspected security vulnerabilities found in our products and solutions. To assist the verification and localization of these vulnerabilities, we have created this template.**

|  |  |  |
| --- | --- | --- |
| **1. Personal or organizational information** | | |
| **name（Optional）** | | **Contact information（Optional）** |
|  | | It is recommended that you leave your contact information for further communication in scenarios such as problem solving. |
| **2.Vulnerability information** | | |
| **Affected Midea Home Appliances UK Ltd. products or components**  We use this information to quickly identify the affected products. Therefore, please provide specific names of the **Midea Home Appliances UK Ltd.** products or components involved. | | |
|  | | |
| **Brief Description of Vulnerability**  Please provide a brief description of the vulnerability, including the type of vulnerability and the potential impact if successfully exploited by an attacker | | |
|  | | |
| **Technical details of the vulnerability**  Please provide technical details of the vulnerability, including the following:  1. Detailed description of the vulnerability technical details.  2. Detailed steps to reproduce the vulnerability (this will be crucial for us to reproduce your findings).  3. If available, a Proof of Concept (PoC) can be attached as an additional file to this report. | | |
|  | | |
| **Description of Vulnerability Exploitation Scenario**  The vulnerability attack scenario is different from the vulnerability reproduction steps. It describes how an attacker successfully exploits the vulnerability, including the prerequisite conditions for the attacker to launch the attack, the triggering limitations of the vulnerability, and whether interaction with the victim is required.  By describing the vulnerability attack scenario, it can help us quickly evaluate your security report, especially for complex security issues. | | |
|  | | |
| **Suggestions for Remediation and Mitigation Measures**  This content can help us with how to fix vulnerabilities, including detailed repair methods, plans, industry best practices, and temporary mitigation measures such as IPS/WAF rule development | | |
|  | | |
| **3.Vulnerability disclosure** | | |
| **Do you have any plans to publicly discuss the vulnerability after it is fixed, including conference speeches or publishing technical articles?**  Please select the appropriate option. We kindly request that you refrain from disclosing the reported security vulnerability to any third party before it is resolved. If you intend to publicly discuss the vulnerability after we have addressed it, such as in conference speeches or technical articles, please contact us at [iotsecurity@midea.com](https://mideasrc.vulbox.com/news/iotsecurity@midea.com). | | |
| YES  NO | | |
| **4.Is it allowed to give external acknowledgement**  **In principle, this vulnerability will be acknowledged in the security notice that is publicly disclosed. Do you agree** | | |
| YES | Please provide the name or nickname for displaying gratitude. | |
| NO |  | |
| **5.Other Information**  Any information that you believe is necessary but not covered in the above information | | |
|  | | |

This strategy description does not constitute a guarantee or commitment, and **Midea Home Appliances UK Ltd.** reserves the right to adjust the strategy mentioned above at its discretion. Please use the information or materials linked in this document at your own risk. **Midea Home Appliances UK Ltd.** reserves the right to change or update this document at any time, and we will update this policy statement as necessary to increase transparency or respond more actively.