**Template for Reporting Suspected Vulnerabilities V01**

**Thank you for reporting suspected vulnerabilities in FIMER products and solutions. Please fill this template in as much detail as possible to help us to verify your information.**

|  |
| --- |
| **1. Individual or Organization Information** |
| **1.1 Contact Information** |
| Please provide contact information so that we can communicate with you for locating faults or in other scenarios. |

…

|  |
| --- |
| **2. Vulnerability Information** |
| **2.1 Affected FIMER Products/Solutions** |
| Please specify FIMER product or component names so that the affected products or components can be quickly located. Please provide to us (if you can identify it):* Product Part Number (from the product label).
* Serial Number (from the product label).
* Firmware Revision (from UI interface if any).
* Interface in use (Ethernet, Wi-Fi).
 |

…

|  |
| --- |
| **2.2 Vulnerability Description** |
| Please provide brief vulnerability information, including the type of vulnerability and the potential impact of successful exploitation. |

…

|  |
| --- |
| **2.3 Technical Details About the Vulnerability** |
| Please provide technical details about the vulnerability, including: * technical information in detail
* procedure for reproducing the vulnerability (which is critical for us to reproduce your findings)
* Proof of Concept (PoC) if possible, which can be sent to us as an additional attachment along with the report.
 |

…

|  |
| --- |
| **2.4 Vulnerability Attack Scenario Description** |
| Please describes how an attacker successfully exploits the vulnerability, including the prerequisites for the attack, trigger conditions, and whether interaction is required. |

…

|  |
| --- |
| **2.5 Recommended Fixes and Mitigations** |
| Please provide detailed fix methods, solutions, industry best practices, and mitigations, which are helpful for vulnerability fixing. |

…

|  |
| --- |
| **3. Vulnerability Disclosure** |
| **3.1 Are you going to publicly discuss the vulnerability (for example, in conference presentations or technical articles for sharing) after the vulnerability is fixed?** |
| Please tick the relevant option, and do not disclose the reported security vulnerability to any third party until it is fixed. If you are going to publicly discuss the vulnerability (for example, in conference presentations or technical articles for sharing) after we fix it, please contact itteb.cybersecurity@fimer.com in advance. |
| [ ] Yes[ ] No |

|  |
| --- |
| **4. Others** |
| Please provide any other information that you deem necessary but is not mentioned above. |

…