**Template for Reporting Suspected Vulnerabilities V1.0**

**Thank you for reporting suspected vulnerabilities in Huawei products and solutions. This template is developed to help you report the suspected vulnerabilities so as to facilitate vulnerability validation and locating.**

|  |  |  |
| --- | --- | --- |
| **1. Individual or Organization Information** | | |
| **(Optional) Name** | | **(Mandatory) Contact Information** |
|  | | Please provide contact information so that we can communicate with you for locating faults or in other scenarios. |
| **2. Vulnerability Information** | | |
| **Affected Huawei Products/Components**  Please specify Huawei product or component names so that the affected products or components can be quickly located. | | |
|  | | |
| **Vulnerability Description**  Please provide brief vulnerability information, including the type of vulnerability and the potential impact of successful exploitation. | | |
|  | | |
| **Technical Details About the Vulnerability**  Please provide technical details about the vulnerability, including (1) technical information in detail; (2) procedure for reproducing the vulnerability (which is critical for us to reproduce your findings); (3) Proof of Concept (PoC) if possible, which can be sent to us as an additional attachment along with the report. | | |
|  | | |
| **Vulnerability Attack Scenario Description**  The vulnerability attack scenario is different from the vulnerability reproduction procedure. It describes how an attacker successfully exploits the vulnerability, including the prerequisites for the attack, trigger conditions, and whether interaction with the victim is required.  This will help us quickly evaluate your security report, especially for complex security issues. | | |
|  | | |
| **Recommended Fixes and Mitigations**  Please provide detailed fix methods, solutions, industry best practices, and mitigations (such as IPS/WAF rule making), which are helpful for vulnerability fixing. | | |
|  | | |
| **3. Vulnerability Disclosure** | | |
| **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 [PSIRT@huawei.com](mailto:PSIRT@huawei.com) in advance. | | |
| Yes  No | | |
| **4. Public Acknowledgment Allowed or Not**  **Can we appreciate you in the security advisory (SA) of the vulnerability?** | | |
| Yes | Please provide the name or nickname that you want to use in the public acknowledgment. | |
| No |  | |
| **5. Others**  Please provide any other information that you deem necessary but is not mentioned above. | | |
|  | | |

The policy described in this document does not constitute warranties or commitments. Huawei may adjust it as appropriate. You use the information in this document or the linked materials at your own risk. Huawei reserves the right to change or update this document at any time as necessary to increase transparency or respond more actively.