**Suspected Vulnerability Report Template**

Thank you for reporting potential security vulnerabilities in our products and solutions. This template is designed to help us quickly verify and locate the issues you've identified.

|  |  |  |
| --- | --- | --- |
| **1. Reporter Information** | | |
| **Name (optional )** | | **Contact information (required)** |
|  | | This will be used to communicate with you for further clarification, issue validation, and updates on remediation progress. |
| **2. Vulnerability Information​** | | |
| **Related products or components affected​**  This information helps us quickly identify affected products. Please provide the exact product/component name. | | |
|  | | |
| **Brief description**  Please describe the vulnerability as briefly as possible, including its type and the possible impacts if successfully exploited by attackers. | | |
|  | | |
| **Technical details** Please provide the technical details of the vulnerability, including: 1. Detailed technical description; 2. Reproduction steps (this information is crucial for us to verify your findings); 3. If available, a Proof of Concept (PoC) – You may include a PoC as an additional attachment along with this report. | | |
|  | | |
| **Attack scenario**  The attack scenario differs from vulnerability reproduction steps—it describes how an attacker could successfully exploit the vulnerability, including prerequisites for attack, vulnerability trigger limitations, victim interaction requirements.  Providing a clear attack scenario description helps us quickly assess your security report, especially for complex security issues. | | |
|  | | |
| **Remediation and Mitigation Recommendations**  This content can help us understand how to fix the vulnerability, including detailed repair methods, solutions, industry best practices, as well as temporary mitigation measures such as IPS/WAF rule configuration. | | |
|  | | |
| **3. Disclosure Preferences** | | |
| **Will you plan to publicly discuss this vulnerability after its remediation, including conference, articles?**  Please select the corresponding option. Note that we require no external disclosure (to any third party other than us) before the reported security vulnerability is fixed. If you intend to publicly discuss the vulnerability after we fix it—including conference, articles, or similar means—please contact our designated official website in advance. | | |
| Yes  No | | |
| **4. Public Acknowledgment**  **For this vulnerability, our security advisory will generally include an acknowledgment of your contribution. Do you consent to this?** | | |
| Yes | Please provide your name or alias. | |
| No |  | |
| **5. Additional Information**  Any information you deem necessary that is not covered in the above sections. | | |
|  | | |

The policy descriptions herein do not constitute any guarantee or commitment. Our company reserves the right to adjust the aforementioned policies at its discretion. All use of information contained in this document or materials linked herein shall be at the user's own risk. Our company retains the right to modify or update this document at any time. We will update this policy statement as necessary to enhance transparency or respond more proactively.