**Suspected vulnerability reporting template v1.0**

**Thank you for the suspected security vulnerabilities in Zowee products and solutions that you will find, and this template is specially formulated to facilitate verification and location of suspected security vulnerabilities.**

|  |  |
| --- | --- |
| **1.** **Personal or Organizational Information** | |
| **Name (optional)** | **Contact (required)** |
|  | It will be used to further communicate with you in scenarios such as problem location |
| **2.** **Vulnerability information** | |
| **Affected Zowee related products or components**  This information is used so that we can quickly locate the affected products, please provide the specific Zowee product or component name. | |
|  | |
| **A brief description of the vulnerability**  Describe the vulnerability briefly as possible, including the type of vulnerability and the possible impact of successful exploitation | |
|  | |
| **Technical details of the vulnerability**  Please provide technical details of the vulnerability, including the following:1il; 2.s); 3.de a PoC (Proof of Concept), you can send it to us as an additional attachment with the report. | |
|  | |
| **Description of the vulnerability attack scenario**  The vulnerability attack scenario is different from the vulnerability reproduction step, which describes how the attacker successfully exploits the vulnerability, including the prerequisites for the attacker to launch the attack, the vulnerability trigger limit, and whether the attacker needs to interact with the victim.  This will help us quickly assess your security reports, especially for complex security issues. | |
|  | |
| **Recommendations for remediation and mitigation measures**  This content can help us how to remediate vulnerabilities, including detailed fixes, solutions, industry best practices, and temporary mitigations such as IPS/WAF rulemaking. | |
|  | |
| **3.** **Vulnerability Disclosure** | |
| **Do you have plans to have a public discussion after the vulnerability is fixed, which can include conference presentations, technical sharing articles, etc.?**  Please select the appropriate option, please select the corresponding option, please note that we ask that you do not disclose the security vulnerability you report to the outside world (this includes any third party other than you) until it has been fixed. If you would like to discuss the vulnerability publicly after we fix it, including conference presentations, technical sharing articles, etc., [please contact PSIRT@brovi.com.cn in advance](mailto:%E8%AF%B7%E6%8F%90%E5%89%8D%E8%81%94%E7%B3%BBPSIRT@brovi.com). | |
| ☐ Yes  ☐ Nope | |
| **4.** **Other Information**  Any information that you deem necessary is not covered in the information above | |
|  | |

The strategy description in this article does not constitute a guarantee or commitment, and Zowee may adjust the above strategy at its discretion. Use of the information in this document or the materials linked to in this document is at your own risk. Zowee 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 be more responsive