**ZTE Security Vulnerability Submission Template**

In order to quickly triage the identified security issue, please fill in the table below correctly:

|  |  |  |
| --- | --- | --- |
| Submitter Information | Nickname |  |
| Unit/Team |  |
| Vulnerability information | **Vulnerability Description (Required)**  *Please specify the vulnerability type, cause, method of exploitation, and potential risk.* | |
|  | |
| **Affected Products (Required)**  *Please provide the product name, module, version, and specific location of the vulnerability.* | |
|  | |
| **Vulnerability Rating (Required)** *Please provide the detailed information of CVSS rating according to your assessment, which can be screenshot or text description.* | |
| Vulnerability Rating: 🞎 Critical 🞎 High 🞎 Medium 🞎 Low  CVSS Score: | |
| **Vulnerability Reproduction Process Description (Required)**  *Please describe the detailed steps required for reproducing the vulnerability by using texts, screenshots, graphics, etc. (recommend to submit a vulnerability reproduction video). If you can provide a POC, please also submit it to us.* | |
|  | |
| **Vulnerability Attack Scenarios**  *Please describe how attackers can successfully exploit vulnerabilities, including the prerequisites and process restrictions of attackers. If you can provide Expoit, please also provide it to us, which will help us quickly analyze vulnerability report.* | |
|  | |
| **Mitigation Suggestions**  *Whether you know how to fix this security vulnerability or have seen best practices in the industry that can help us fix and solve this vulnerability.* | |
|  | |

**Notes**: As security vulnerabilities are sensitive information, we strongly suggest you report ZTE-related security vulnerabilities to ZTE PSIRT (psirt@zte.com.cn) and use our PGP public key to encrypt the sensitive information.

**POC/Exploit Requirements:**

*(1) Providing a complete POC or Exploit, which can be used to successfully verify the reported vulnerability.*

*(2) Compilation and running environment description, including: compiler name, compiler version, compilation options, operating system version, and other necessary information.*

*(3) The running result of POC or Exploit should be consistent with that described in your report.*