# 中兴通讯安全漏洞提交模板

**非常感谢您对中兴通讯产品的关注，并愿意将您发现的安全漏洞提交给我们。**

**为更快速地验证和定位漏洞，请您按照如下表格填写相关内容。**

|  |  |  |
| --- | --- | --- |
| ****提交人信息**** | ****网络名称**** |  |
| ****单位/团队**** |  |
| ****漏洞信息**** | ****漏洞描述（必填）*****需包含漏洞类型、产生原因、利用方式、漏洞可能造成的安全风险等信息。* |
|  |
| ****受影响产品（必填）*****请您提供详细的产品名称、模块信息、版本信息、具体的漏洞位置等。* |
|  |
| ****漏洞评级（必填）*****请您提供CVSS自评详细信息，可截图或文字描述。* |
| **自评漏洞级别：🞎严重 🞎高危 🞎中危 🞎低危****CVSS得分：** |
| ****漏洞复现过程描述（必填）*****请您采用文字、截图、图形等方式，按步骤详细阐述漏洞复现过程（推荐提交漏洞复现视频）,如您可提供POC，也请一并提交给我们。* |
|  |
| ****漏洞攻击场景介绍*****请您阐述攻击者如何成功利用漏洞，包括攻击者攻击的前提条件、过程限制等信息，如您可提供Expoit，也请一并提供给我们，对我们快速分析漏洞报告会有所帮助。* |
|  |
| ****修复建议*****对此安全漏洞，您是否了解其修复方法，或者您是否看到过业界最佳实践等，可以帮助我们更好地修复解决此问题。* |
|  |

****特别提醒：**由于安全漏洞属于敏感信息，强烈建议使用中兴通讯的PGP公钥进行加密，直接发送至psirt@zte.com.cn。**

**说明：**

****POC/Exploit要求****

1. *完整可编译的POC或Exploit，可使用POC或Exploit成功验证提交的漏洞。*
2. *编译和运行环境说明，需包括：编译器名称，编译器版本，编译选项以及操作系统版本等必要信息。*

*（3）POC或者Exploit的运行结果应该与报告描述一致。*