**疑似漏洞上报模板**

**感谢您将发现的我公司产品和解决方案中的疑似安全漏洞上报给我们，为便于验证和定位疑似安全漏洞，特制定本模板。**

|  |
| --- |
| **1.个人或组织信息** |
| **姓名（可选）** | **联系方式（必填）** |
|  | 将用于在问题定位等场景下，与您进行进一步的交流 |
| **2.漏洞信息** |
| **受影响的相关产品或组件**此信息用于我们可以快速定位受影响的产品，请提供具体的产品或组件名称。  |
|  |
| **漏洞简要描述**请尽量简要描述该漏洞，包括漏洞类型和攻击者成功利用该漏洞可能带来什么影响 |
|  |
| **漏洞技术细节**请提供该漏洞的技术细节，包括以下内容：1.详细描述漏洞技术细节；2.漏洞复现详细步骤（此内容这将对于我们复现您的发现至关重要）；3.如果您可以提供PoC（概念验证），可以作为额外的附件与该报告一同发给我们。 |
|  |
| **漏洞攻击场景描述**漏洞攻击场景不同于漏洞复现步骤，它描述的是攻击者如何成功利用该漏洞，它包括了攻击者发起攻击的前提条件，漏洞触发限制，是否需要与受害者交互等内容。通过漏洞攻击场景描述，这会帮助我们快速的评估您的安全报告，特别是针对复杂的安全问题。 |
|  |
| **修复及缓解措施建议**此内容可以帮助我们如何修复漏洞，包括详细修复方法，方案，业界最佳实践以及临时缓解措施如IPS/WAF规则制定等。 |
|  |
| **3.漏洞披露** |
| **您是否有计划待该漏洞修复后进行公开讨论，这包括会议演讲，发表技术分享文章等？**请您选择对应的选项，请注意我们要求在您上报的安全漏洞被修复之前，不要对外披露（这包括除您之外的任何第三方）。若您打算在我们修复漏洞之后公开讨论漏洞，这包括会议演讲，发表技术分享文章等，请提前联系我们指定的官网。 |
| [ ] 是[ ] 否 |
| **4.是否允许对外致谢****此漏洞在对外披露的安全通告中会原则上会增加对您的致谢，是否同意** |
| [ ] 是 | 请提供致谢的显示姓名或昵称 |
| [ ] 否 |  |
| **5.其它信息**您认为必要的不在上面信息中涵盖的任何信息 |
|  |

本文的策略描述不构成保证或承诺，我公司可酌情对上述策略进行调整。对本文档中的信息或文档链接的材料使用的请做好风险自担。我公司公司保留随时更改或更新本文档的权利，我们会在必要时更新本策略说明以增加透明度或更加积极地响应。