# 看雪二进制漏洞分析文章基础模板

## 一、漏洞信息

### 1. 漏洞简述

（必有）

* 漏洞名称：（中文）
* 漏洞编号：（CVE编号）
* 漏洞类型：（整数溢出、UAF、设计缺陷等）
* 漏洞影响：（远程代码执行、信息泄露等）
* CVSS评分：（以CVSS 3.0为准（一般分数较高），或者2者都备注）
* 利用难度：Medium
* 基础权限：不需要（是否需要普通用户权限）

### 2. 组件概述

如果是操作系统组件，简单介绍组件的大概情况：是什么，用处，用在什么地方，使用范围等。

### 3. 漏洞利用

简述漏洞利用过程和成功利用的效果，精简凝练。

### 4. 漏洞影响

漏洞影响的详细软件或操作系统版本。

### 5. 解决方案

官方的安全更新方案，给出链接。

## 二、漏洞复现

（必有）

### 1. 环境搭建

* 靶机环境版本详述
* 靶机配置
* 攻击机环境版本详述
* 攻击机配置

### 2. 复现过程

分1，2，3步骤详述漏洞的复现过程。

## 三、漏洞分析

### 1. 基本信息

* 漏洞文件：存在漏洞的具体文件名
* 漏洞函数：存在漏洞的具体函数名
* 漏洞对象：触发漏洞的结构或其他数据对象

### 2. 背景知识

该部分内容主要简介漏洞分析过程中所使用到的相关知识，丰富程度由个人决定。

### 3. 详细分析

#### 1. 基础分析

根据漏洞复现结果获取的一手信息的简单分析，例如根据crash的栈回溯情况推测出的可能出问题的位置，根据官网漏洞信息或公开漏洞信息获取到的漏洞的基础分析结果。

备注清晰需要使用的文件的详细版本，以防其他人复现分析时因为版本问题踩坑。

#### 2. 静态分析

（必有）

纯静态分析内容，动静结合的可以放在动态分析过程中。

##### 1. 函数调用链

可以是正向的函数调用，也可以是逆向的函数追踪。

##### 2. 补丁Diff

如果有补丁diff，最好能给出补丁diff的详细分析。（知道怎么攻，也要知道怎么防。）

##### 2. 漏洞函数分析

具体的漏洞函数功能、触发条件、源代码分析

#### 3. 动态分析

（可选）

详细动态调试信息

### 4. 利用思路

（可选）

##### 1. 利用条件

漏洞利用的必备条件：场景、配置、操作等

##### 2. 利用过程

攻击过程升级版，最好是结合流程图，更为清晰。

##### 3. 攻击向量

该漏洞可能存在的攻击向量。

## 四、缓解措施

（可选）

官方或已公开的经过验证的漏洞缓解措施。

## 五、参考文献

（必有）

文章的参考文献或个人博客。