# 处理一个CVE漏洞

## CVE漏洞

CVE全称为Common Vulnerabilities and Exposures，公共漏洞和暴露，又称通用漏洞披露、常见漏洞与披露，是一个与信息安全有关的数据库，收集各种信息安全弱点及漏洞并给予编号以便于公众查阅。此数据库现由美国非营利组织MITRE所属的National Cybersecurity FFRDC所营运维护。

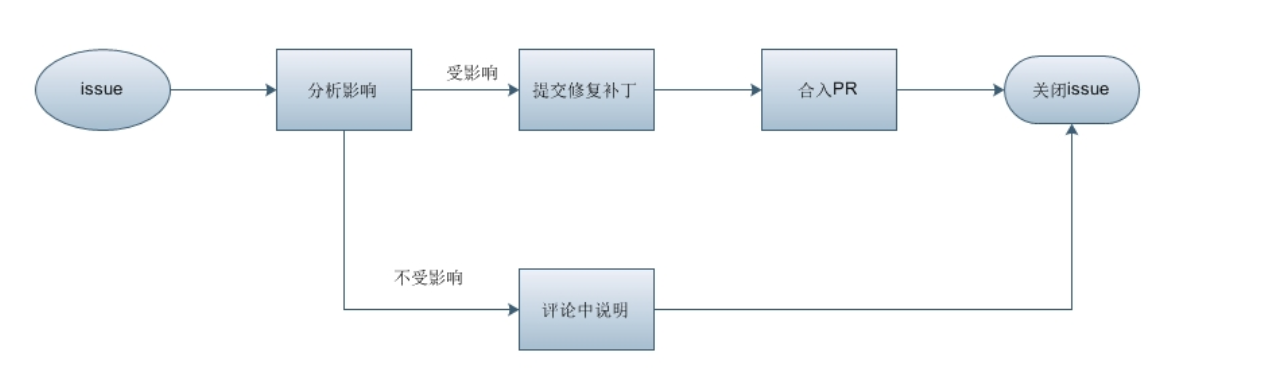
CVE对每一个漏洞都赋予一个专属的编号，格式为CVE-YYYY-NNNN。其中YYYY为年份，NNNN为CVE的编号，例如CVE-2020-11945。

openEuler的CVE信息来源为NVD，NVD是一个美国政府基于安全内容自动化协议（SCAP）标准的漏洞管理数据的存储库，可实现漏洞管理、安全性度量和合规性的自动化。NVD的官方网址为<https://nvd.nist.gov/> 。

漏洞严重程度通常通过CVSS来衡量，CVSS是一个开放框架，用于传达软件漏洞的特征和严重性。CVSS由三个度量标准组组成：基础，时间和环境。基本指标产生的分数介于0到10之间，然后可以通过对时间和环境指标进行评分来进行修改。openEuler根据CVSS评分将漏洞严重程度分为四个等级：严重——9分以上，主要——7.0 – 8.9分，次要——4.0 – 6.9，不重要——0.1 – 3.9。

openEuler安全委员会（Security Committee, SC）过接收和响应openEuler产品安全问题报告、提供社区安全指导，开展安全治理等活动提升社区产品的安全性。SC在openEuler社区官网发布了漏洞管理策略，包括如何上报安全问题、获取SA和安全补丁等信息，详见 https://openeuler.org/zh/security/vulnerability-reporting/

下图为处理CVE漏洞的流程：



本文以squid的漏洞CVE-2020-11945（issue链接：<https://gitee.com/angela7/squid/issues/I3HY8O>）举例说明处理CVE漏洞的流程。

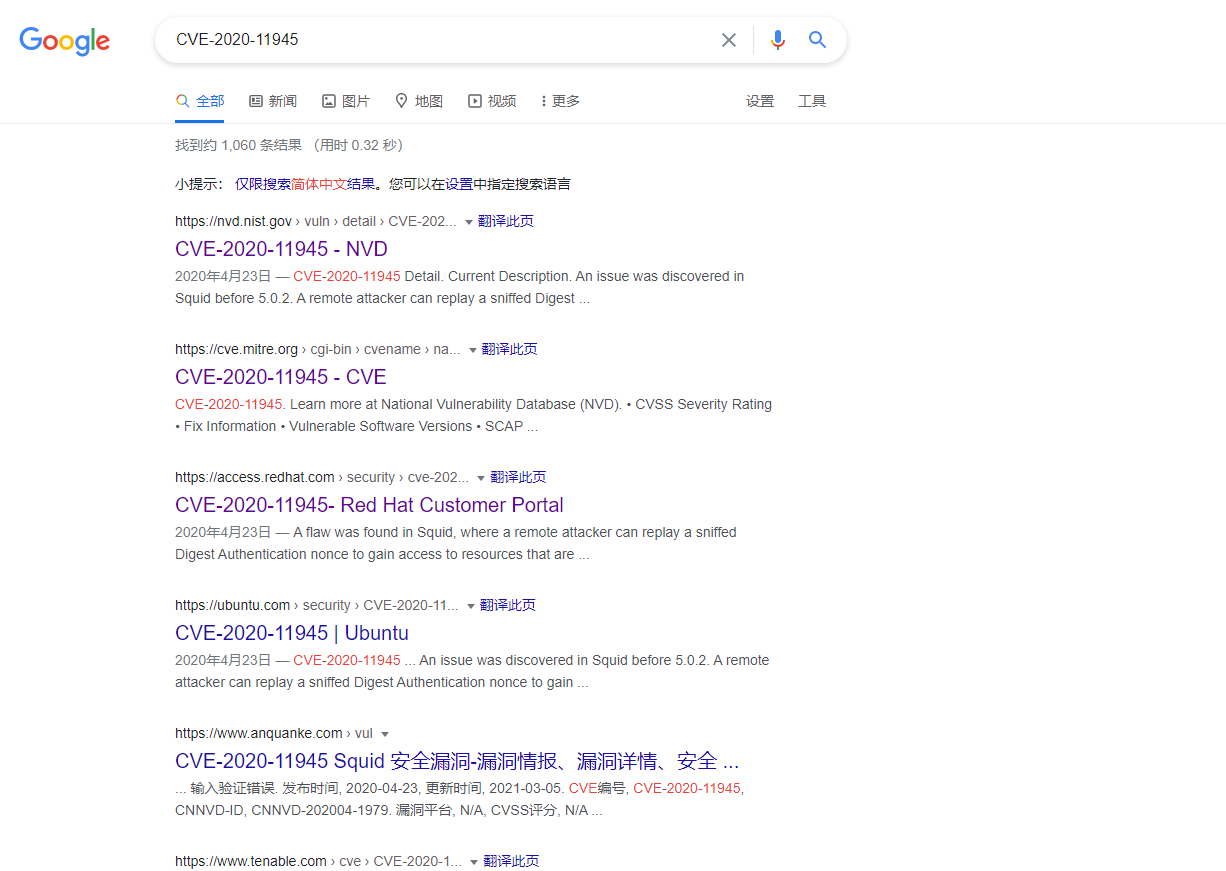
分析影响

## 2.解决CVE漏洞

小技巧：

CVE信息可通过网络搜索CVE号获取更多信息，包括官网链接以及相关文档分析，例如相关组件上游社区、nvd等网站给出的信息。当然，查找的资料越多，越有助于我们理解漏洞的攻击原理和主要影响。在漏洞描述中我们可以找到漏洞影响组件版本，再对比openEuler上相关组件判断是否受影响。如受影响则需要提交PR合入修复补丁；不受影响在评论里说明即可，不需要合入PR。

1. 通过网络搜索CVE号，获取更多信息。



1. 分析影响

通过查找相关资料，nvd(https://nvd.nist.gov/vuln/detail/CVE-2020-11945)对该漏洞的描述为：An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).

理解分析一下，该漏洞影响为：远程攻击者可以重播嗅探到的摘要身份验证随机数，以获取对原本禁止的资源的访问。这种情况是由于攻击者可能使随机数引用计数器溢出，如果释放了合并的令牌凭据，就会导致远程执行代码。nvd清楚地写明了该漏洞影响squid版本为5.0.2之前的版本。而openEuler社区版本为4.9，则该漏洞为受影响漏洞，需要提交PR修复。且该漏洞的评分为9.8分，为严重漏洞。

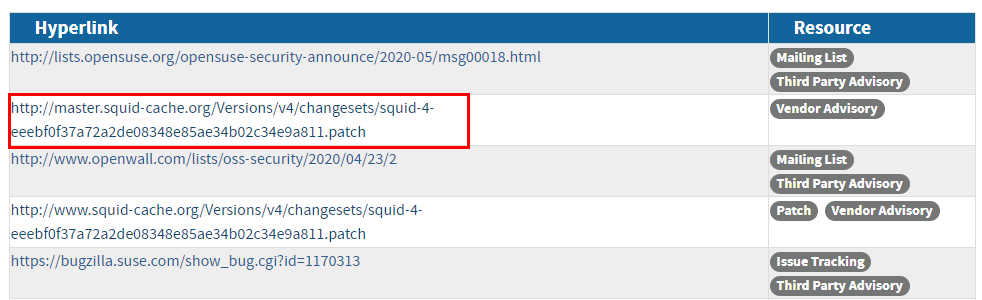
1. 提交PR

如果CVE影响版本，则需要提交修复补丁。提交修复补丁需要从上游社区获取补丁，可能需要进行代码适配。提交补丁时需要注意PR描述信息中关联对应issue编号，修改spec文件中的release号和changelog信息。

小技巧：

一般情况下，修复补丁链接会在相关分析文档中体现。

例如：squid的漏洞CVE-2020-11945，nvd在附加链接里已经附上了上游社区的补丁链接。

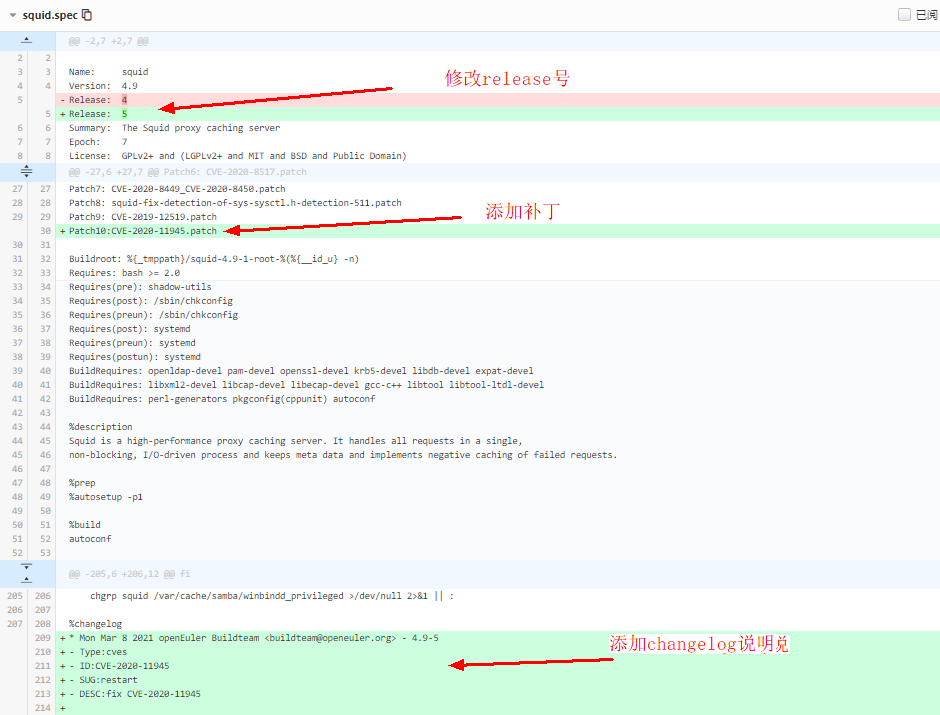


上游社区补丁的下载链接 <http://www.squid-cache.org/Versions/v4/changesets/squid-4-eeebf0f37a72a2de08348e85ae34b02c34e9a811.patch>

PR提交指导文档参考<https://gitee.com/openeuler/community/blob/master/zh/contributors/pull-request.md>

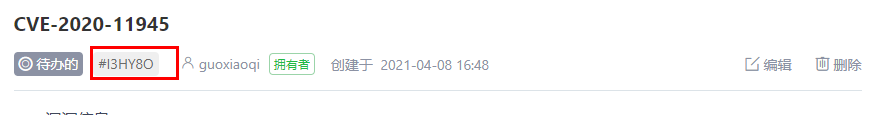
按照文档中的步骤将该补丁提交PR，可参考PR提交：<https://gitee.com/src-openeuler/squid/pulls/16>

spec的修改参考截图：

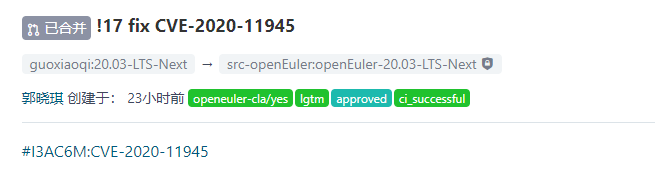


ps：由于该包的spec的%prep阶段使用了%autosetup，因为无需在%prep阶段执行打补丁的操作，补丁就会自动被读取并打上。

关联PR，在PR描述中添加issue号，issue号位置参考截图



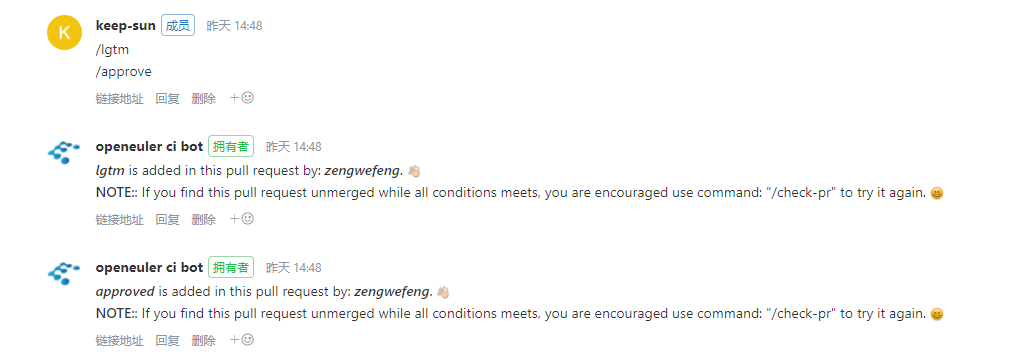
PR中关联issue号例子：



1. 合入PR

等待审核代码提交，合入PR或提出检视意见，如果有检视意见，需要修改后再次提交。在此期间，可以通过评论的方式与社区人员进行沟通。

例如：



5. 关闭issue

如果你已经完成了上述步骤，就可以关闭issue了，感谢你为我们操作系统修复了一个安全漏洞，降低了攻击者入侵系统的概率。

关闭方法为评论/hdc-completed，随后会有专人审核你处理得是否正确。