漏洞编号:CVE-2021-21686

漏洞来源:

平台：CVE/NVD

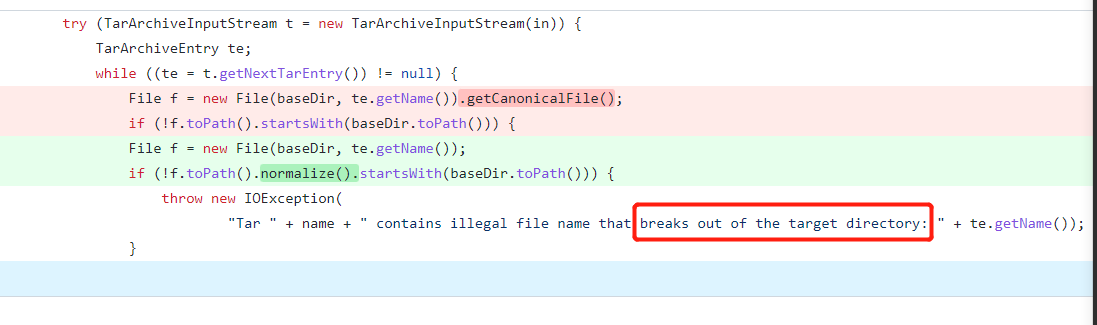
连接：https://nvd.nist.gov/vuln/detail/CVE-2021-21686

漏洞披露时间:11/04/2021

野外漏洞报告：

<https://www.cvedetails.com/cve/CVE-2021-21686>

漏洞成因:



文件过滤器没有规范路径允许与外部文件创建符号链接

漏洞位置:

core/src/main/java/hudson/FilePath.java 第2840行

漏洞PoC：无

漏洞补丁：

https://github.com/jenkinsci/jenkins/pull/5900/files

漏洞类型：

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

漏洞危害：这可能允许攻击者读写Jenkins控制器文件系统上的任意文件。

漏洞评级：8.1HIGH

影响版本（网站）：

**1.408.1-2.303.2**

**<2.318**

漏洞修复版本：2.303之后

漏洞描述：代理到控制器的安全子系统限制了代理进程可以访问Jenkins控制器上的哪些文件。文件路径过滤器不规范化路径，允许操作遵循符号链接到允许的外部目录。

漏洞处置建议：建议升级到2.303.2之后，或者直接修改相应位置代码

漏洞参考链接：https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455

https://github.com/jenkinsci/jenkins/pull/5900/files