漏洞编号: cve-2021-21687

漏洞来源:

平台： cve/nvd

连接：https://nvd.nist.gov/vuln/detail/CVE-2021-21687

漏洞披露时间:11/04/2021

野外漏洞报告：https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2021-21687

漏洞成因: FilePath#untar 在取消归档符号链接时不检查创建符号链接的权限。

漏洞位置: core/src/main/java/hudson/FilePath.java 中581行，569行

漏洞PoC：无

漏洞补丁：https://github.com/jenkinsci/jenkins/pull/5885/files中对于FilePath的修改

漏洞类型：[CWE-862](http://cwe.mitre.org/data/definitions/862.html" \t "https://nvd.nist.gov/vuln/detail/_blank) Missing Authorization

漏洞危害: 这可能允许攻击者获得对 Jenkins 控制器文件系统上任意文件的读写权限

漏洞评级：9.1 critical

影响版本（网站）：

1.408.1-2.303.2

2.319之前

漏洞修复版本：

2.303.3之后

漏洞描述：Jenkins 2.318 及更早版本、LTS 2.303.2 及更早版本在取消归档 FilePath#untar 中的符号链接时不检查代理到控制器的访问以创建符号链接。

漏洞处置建议：请升级至2.303.3版本以上

漏洞参考链接：

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：  
https://www.jenkins.io/security/advisory/2021-11-04/#SECURITY-2455