漏洞编号: CVE-2021-44224

漏洞描述:

漏洞来源: 平台 NVD

链接 https://nvd.nist.gov/vuln/detail/CVE-2021-44224

漏洞披露时间: 12/20/2021

漏洞参考链接:

野外漏洞报告：<https://cert.360.cn/warning/detail?id=9eddce1b5120cc0b0ec423f17aaf2940>

漏洞类型: [CWE-476](http://cwe.mitre.org/data/definitions/476.html" \t "https://nvd.nist.gov/vuln/detail/_blank)

漏洞危害: 空指针取消引用

漏洞严重性:

CVSS 3.x评分：8.2

CVSS 2.0 评分：6.4

漏洞影响的组件版本:

apache:http\_server 2.4.7-2.4.52

tenable:tenable.sc 5.14.0-5.20.0； 5.16.0-202201.1

apple:macos 11.0-11.6.6； 12.0.0-12.4

漏洞修复的组件版本:

漏洞成因:

如果httpd 配置作为转发代理（ProxyRequests on） ，可允许攻击者通过精心构造的 URI ，导致崩溃（空指针取消引用），或者如果httpd的配置为混合转发和反向代理声明，可以允许攻击者将请求发送到声明的 Unix 域套接字端点，造成服务器端请求伪造。

漏洞位置:

未知

漏洞PoC：

https://www.h3c.com/cn/d\_202112/1519672\_30003\_0.htm

漏洞补丁：https://bugzilla.redhat.com/show\_bug.cgi?id=2034672

漏洞处置建议：