关于Apache HTTP Server（CVE-2021-44224、CVE-2021-44790）多个漏洞风险提示

漏洞相关 吴昊A 2021-12-24 发表

漏洞相关信息

漏洞编号： CVE-2021-44224、CVE-2021-44790

漏洞名称： Apache HTTP Serve

产品型号及版本： A2000-G SMP Comware V5 V7平台安全设备 CSAP-SA

漏洞描述

【关于Apache HTTP Server多个漏洞风险提示】 一、背景介绍 12月23日，市委网信办技术支撑单位监测到Apache官方发布了关于Apache HTTP Server存在SSRF漏洞及缓冲区溢出漏洞的安全通告，涉及多个高危漏洞（CVE-2021-44224、CVE-2021-44790） 1.1 部分漏洞详细介绍： CVE-2021-44224漏洞: 发送到配置为转发代理（ProxyRequests on）的 httpd 的精心制作的 URI 可能导致崩溃（空指针取消引用），或者对于混合转发和反向代理声明的配置，可以允许将请求定向到声明的 Unix 域套接字端点,造成服务器端请求伪造。 CVE-2021-44790漏洞: 设计的请求正文可能会导致 mod_lua 多部分解析器（从 Lua 脚本调用的 r:parsebody()）中的缓冲区溢出，并导致在目标系统上执行任意代码。该漏洞无需经过身份验证即可被远程利用。 1.2 漏洞编号 CVE-2021-44224 CVE-2021-44790 1.3 漏洞等级 高危 二、修复建议 2.1 受影响版本 CVE-2021-44224：Apache HTTP Server>=2.4.7, <=2.4.51 CVE-2021-44790：Apache HTTP Server<=2.4.51 2.2 修复建议 官方已经发布了解决此漏洞的软件更新，建议受影响用户尽快升级到安全版本。 官方链接：https://httpd.apache.org/download.cgi

漏洞解决方案

均不涉及该漏洞