

知

SecPath F1000-AK1414 是否涉及nginx越界写入漏洞（CVE-2022-41742）

漏洞相关

zhiliao_nHokMf

2023-11-15 发表

漏洞相关信息

漏洞编号：CVE-2022-41742

漏洞名称：nginx越界写入漏洞

产品型号及版本：SecPath F1000-AK1414

漏洞描述

nginx越界写入漏洞

nginx 越界写入漏洞 (CVE-2022-41742)	
受影响主机	10.26.44.240; 点击查看详情;
详细描述	此插件基于版本检测，有可能误报。 Nginx是美国Nginx公司的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。 Nginx Plus 的模块 ngx_http_hls_module 中存在一个漏洞，该漏洞可能允许本地攻击者破坏 NGINX 的工作进程内存，从而导致其崩溃或使用特制的音频或视频文件时产生其他潜在的影响。只有当配置文件中使用 hls 指令时，该问题才会影响 Nginx Plus。 此外，只有当攻击者可以触发使用模块 ngx_http_hls_module 对特制音频或视频文件进行处理时，攻击才有可能成功。一次成功的利用可能允许一个本地攻击者破坏 NGINX 的 worker 进程，导致其中止或其他潜在的影响。 https://mailman.nginx.org/pipermail/nginx-announce/2022/RBRRON6PYBJJM2XIAPQBFBVLR4Q6IHRA.html

漏洞解决方案

没有使用该组件，comware防火墙不涉及此漏洞问题。

