CloudOS是否涉及nginx 安全漏洞(CVE-2021-23017)

郑博之 2021-11-13 发表

漏洞相关信息

漏洞编号： CVE-2021-23017

漏洞名称： nginx 安全漏洞，也即 Nginx DNS Resolver中的一个任意代码执行漏洞

产品型号及版本： Cloud OS2.0&3.0&5.0

漏洞描述

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存在安全漏洞，该漏洞源于一个离一错误在该漏洞允许远程攻击者可利用该漏洞在目标系统上执行任意代码。

这个漏洞的触发机制如下：

5月26日，Nginx发布安全公告，修复了nginx解析器中的一个DNS解析程序漏洞（CVE-2021-23017），由于ngx_resolver_copy()处理DNS响应时存在错误，当nginx配置文件中使用了“ resolver”指令时，未经身份验证的攻击者能够伪造来自DNS服务器的UDP数据包，构造特制的DNS响应导致1字节内存覆盖，从而造成拒绝服务或任意代码执行。

漏洞解决方案

1、CloudOS 2.0、3.0 以及5.0的 5103 之前，不涉及该漏洞。
不涉及原因：CloudOS的nginx未使用相关的配置，虽然nginx版本属于受漏洞影响的版本中，但是没有相关配置，不会触发相关的漏洞。

2、CloudOS 5.0的5103 至5132P01之前涉及该漏洞。
解决方法：升级至5132P01及之后版本，后续版本里升级了nginx组件。

3、CloudOS 5.0的 5132P01及之后版本不涉及该漏洞。
不涉及原因：已升级nginx组件。