Citrix SD-WAN 被曝远程代码执行漏洞

转载

奇安信代码卫士 于 2020-11-17 17:31:55 发布 372 收藏
文章标签： 网络 安全 信息安全 物联网 区块链

聚焦源代码安全，网罗国内外最新资讯！

编译：奇安信代码卫士团队

研究人员指出，Citrix 软件定义 (SD)-WAN 平台可导致远程代码执行后果和网络接管后果。

这些缺陷影响 Citrix SD-WAN 中心（11.2.2、11.1.2b 和10.2.8之前的所有版本），是一个存在于 stop_ping 中的未认证路径遍历和 shell 注入漏洞 (CVE-2020-8271)、一个 ConfigEditor 认证绕过漏洞 (CVE-2020-8272) 和一个 CreateAzureDeployment shell 注入漏洞 (CVE-2020-8273)。它们的严重性评分尚未公开。

在前两个漏洞案例中，攻击者必须能够和 SD-WAN 中心的管理 IP 地址或全限定域名 (FQDN) 通信，而第三个漏洞攻击者需要认证。

漏洞概述

CVE-2020-8271 可使攻击者利用 Citrix SD-WAN 中心中的根权限实现未认证 RCE。Realmode Labs 已发布相关 writeup 详情指出，“ /collector/diagnostics/stop_ping 端点读取文件 /tmp/pid_ 。$req_id 使用在 shell_exec 调用中的内容。针对用户提供的 $req_id 未执行任何检查，从而导致路径遍历问题。有人可以在任何地方释放含有用户控制内容的文件（例如，使用 /collector/licensing/upload） 并运行任意 shell 命令。”

CVE-2020-8272 漏洞和 CakePHP 将 URI 转化为端点函数参数有关，可导致 SD-WAN 功能遭未认证暴露。Citrix SD-WAN 基础设施在 Apache 上运行，以CakePHP2 为框架。研究人员从 CakePHP2 框架处理 URL 的方式中发现了一个漏洞。为此，Citrix 公司在 CakeRequest.php 中使用了函数 “_url。

研究人员指出，“如果我们的 REQUEST_URI 中在 URI 开头的 :// 后包含 ?，则会被删除。它将导致 Apache 如何看待 URI 和 CakePHP 如何分析之间存在差异，从而使我们绕过对 Collector 端点的客户端证书检查。” 例如，格式为 “aaaaaaaaaaaaaaaa/:///?/collector/diagnostics/stop_ping” 的 URI 将转换为 /collector/diagnostics/stop_ping 且不要求客户端证书或认证。这就导致未认证攻击者访问 ConfigEditor 功能。

至于第三个漏洞 CVE-2020-8273，用户提供的数据通过 JSON 编码并通过该代码拼接为一个 exec 调用。研究人员表示，“确实难以预测到 CakePHP 对待 URL 的方式。这就是为何对产品执行专门的安全审计如此重要的原因。”

SD-WAN 漏洞在增多

上周，Realmode Labs 披露了位于 Silver Peak Unity Orchestrator for SD-WAN 中的三个远程代码执行漏洞。未认证攻击者可组合利用这些漏洞实现网络接管。研究人员指出它们还曾在另外两个 SD-WAN 平台上找到类似缺陷，目前已修复，后续将披露。

SD-WAN 是一款基于云的网络方法，适用于各种规模的企业和跨地区公司。它允许各地区和云实例通过各种连接方式相互连接和连接到公司资源，并通过软件控制来管理该流程，包括资源和节点的协调。

SD-WAN 的市场份额正在增长，同时也引起了网络犯罪分子的兴趣。遗憾的是，顶级 SD-WAN 供应商在过去也曾发现过多种问题。

例如，今年3月份，Cisco Systems 修复了三个高危漏洞。它们可导致本地认证攻击者以 root 权限执行命令。一个月之后，思科 IOS XE 中也发现了类似漏洞。去年12月，Citrix Application Delivery Controller (ADC) 和 Citrix Gateway 产品中被曝一个严重的 0day，可导致设备遭接管和 RCE 后果。该 0day 公布后，立即出现了在野攻击活动中，且 exploit 遭公开。

推荐阅读

Citrix 修复严重漏洞，可导致 XenMobile Server 遭接管

思杰修复网络产品中的11个漏洞

思杰 ShareFile 被曝多个漏洞，可导致企业机密被盗

原文链接

https://threatpost.com/citrix-sd-wan-bugs-remote-code-execution/161274/

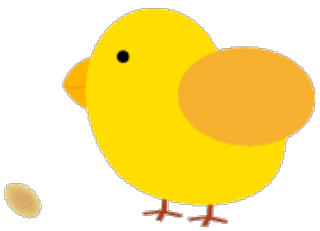
题图：Pixabay License

本文由奇安信代码卫士编译，不代表奇安信观点。转载请注明“转自奇安信代码卫士 https://codesafe.qianxin.com”。

奇安信代码卫士 (codesafe)

国内首个专注于软件开发安全的

产品线。



觉得不错，就点个“在看”或"赞”吧~