CNVD 安全漏洞信息具体情况

漏洞名称	漏洞中文描述	CVE 编号	漏洞影响对象类型	产品	修复版本	最早公开时间	安全建议	攻击途径	攻击复杂度
云科 YK-ADC 高级 Web 应用防护系统模块 DNS 查询拒绝服务漏洞	云科 YK-ADC 是集成了网络流量编排、负载均衡、智能 DNS，Web 应用防护、远程接入策略管理等功能的应用交付平台。 YK-ADC 高级 Web 应用防护系统模块是（配置在启用服务器端请求伪造(SSRF)防护的虚拟服务器）存在拒绝服务漏洞。该漏洞产生的原因是未公开的请求会干扰新的客户端请求，导致流量中断。攻击者可利用该漏洞远程、未认证地对受影响系统发起拒绝服务(DoS)攻击。	CVE-2025-58474	网络设备（交换机、路由器等网络端设备）	YK-ADC 容翼系列	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 27 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 高级 Web 应用防护系统模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 高级 Web 应用防护系统模块存在拒绝服务漏洞。该漏洞产生的原因是当安全策略配置了长度超过 1024 字符的 URL（无论是手动还是通过自动策略生成器），会导致 bd 进程反复终止。攻击者可利用该漏洞，通过自动策略生成器触发长 URL 配置，造成受影响系统的拒绝服务（DoS），导致流量中断。	CVE-2025-61938	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 高级 Web 应用防护系统模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 高级 Web 应用防护系统模块在配置了包含格式错误的 JSON schema 的 JSON 内容配置文件，并将安全策略应用于虚拟服务器时，存在拒绝服务漏洞。该漏洞产生的原因是安全策略中的 JSON schema 格式错误，导致在接收到未公开的请求时，bd 进程会终止。攻击者可利用该漏洞远程、未认证地触发 bd 进程崩溃，造成 YK-ADC 系统流量中断，发起拒绝服务攻击。	CVE-2025-54858	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 高级 Web 应用防护系统模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 高级 Web 应用防护系统模块存在拒绝服务漏洞，该漏洞产生的原因是当安全策略配置在虚拟服务器上时，未公开的请求可能导致 bd 进程终止。攻击者可利用该漏洞发起拒绝服务攻击。	CVE-2025-61935	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC AFM 拒绝服务防护配置拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC AFM 的拒绝服务（DoS）防护配置模块存在拒绝服务漏洞。该漏洞产生的原因是当在虚拟服务器上配置 DoS 防护配置文件时，未公开的请求可能导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-59478	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC APM 和 SSL 流量编排拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC APM 和 SSL 流量编排模块存在拒绝服务漏洞。该漏洞产生的原因是当系统的 SAML 服务提供者（SP）与身份提供者（IdP）模块在启用单点注销（SLO）功能时，未公开的请求会导致内存资源利用率增加。攻击者可利用该漏洞发起拒绝服务攻击。	CVE-2025-47148	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC APM 跨站脚本漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC APM 的某个未公开页面存在跨站脚本漏洞，该漏洞产生的原因是页面未正确处理用户输入，导致恶意代码被反射执行。攻击者可利用该漏洞诱使用户访问特制的 URL，从而在目标用户的浏览器上下文中执行任意 JavaScript 代码。	CVE-2025-61933	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC APM 门户访问模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC APM 的门户访问模块存在拒绝服务漏洞。该漏洞产生的原因是当在 YK-ADC APM 门户访问虚拟服务器上配置了按请求策略时，未公开的流量可能导致流量管理微内核进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-61960	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC APM 访问策略管理模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC APM 的访问策略管理模块存在拒绝服务漏洞，该漏洞产生的原因是当在虚拟服务器上配置访问策略时，未公开的流量可能导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞造成 YK-ADC APM 系统的拒绝服务。	CVE-2025-53521	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC APM OAuth 访问配置文件拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC APM 的 OAuth 访问配置文件存在拒绝服务漏洞。该漏洞产生的原因是当在虚拟服务器上配置了 OAuth 访问配置时，未公开的流量可能导致 apmd 进程终止。攻击者可利用该漏洞发起拒绝服务攻击。	CVE-2025-54854	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 配置工具目录遍历漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 配置工具存在目录遍历漏洞。该漏洞产生的原因是认证攻击者可通过发送特制请求，访问未被限制的文件路径。攻击者可利用该漏洞访问超出预期目录范围的任意文件，造成敏感信息泄露等安全风险。	CVE-2025-54755	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 配置工具信息泄露漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 配置工具的某些未公开端点存在信息泄露漏洞。该漏洞产生的原因是这些端点包含静态的非敏感信息，且可被未认证的远程攻击者通过配置工具访问。攻击者可利用该漏洞在具备网络访问权限的情况下，通过管理端口或 self IP 地址访问不包含设备专属或配置信息的页面，从而获取静态非敏感信息。	CVE-2025-59268	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 配置工具任意文件上传漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的配置工具存在任意文件上传漏洞，该漏洞产生的原因是配置工具的某个未公开 URL 存在安全缺陷，允许高权限认证攻击者上传任意文件。攻击者可利用该漏洞上传恶意文件，可能导致系统安全受到威胁。	CVE-2025-59483	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 配置工具跨站脚本漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 配置工具的某个未公开页面存在跨站脚本漏洞，该漏洞产生的原因是攻击者可以存储恶意 HTML 或 JavaScript 代码在配置工具中。攻击者可利用该漏洞在当前登录用户的上下文中执行 JavaScript 代码，若受害者为具有高级 Shell（bash）权限的管理员用户，攻击者可进一步危害 YK-ADC 系统安全。	CVE-2025-59269	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 产品 DNS 缓存拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 产品的 DNS 缓存模块存在拒绝服务漏洞，该漏洞产生的原因是配置 DNS 缓存时，未公开的 DNS 查询可能导致内存资源利用率增加。攻击者可利用该漏洞造成拒绝服务影响。	CVE-2025-59781	网络设备（交换机、路由器等网络端设备）	YK-ADC##YK-ADC NextCNF	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC DTLS1.2 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 DTLS1.2 虚拟服务器存在拒绝服务漏洞。该漏洞产生的原因是当虚拟服务器启用 Server SSL 配置证书、密钥且 SSL 签名哈希设置为 ANY，且后端服务器启用 DTLS1.2 和客户端认证时，未公开的流量可导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞导致 YK-ADC 系统 TMM 进程重启，造成流量中断。	CVE-2025-61951	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC HSB 锁死漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 HSB 模块存在锁死漏洞，该漏洞产生的原因是在未公开的流量条件以及攻击者无法控制的其他条件下，HSB 可能会发生锁死。攻击者可利用该漏洞导致流量中断，直到手动干预或 TMM（Traffic Management Microkernel）检测到锁死并重启为止。	CVE-2025-58153	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	高

云科 YK-ADC HTTP/2 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 AdvancedWAF 和 ASM 安全策略模块在配置服务端 HTTP/2 配置文件时，存在拒绝服务漏洞。该漏洞产生的原因是未公开的流量可导致流量管理微内核（TMM）异常终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-55669	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 权限提升漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 iControl REST 和 TMOS Shell（tmsh）模块存在权限提升漏洞，该漏洞产生的原因是认证后的攻击者（至少具备资源管理员角色）可通过受影响的 iControl REST 接口或本地 tmsh 命令，执行具有更高权限的系统命令，进而绕过安全边界。攻击者可利用该漏洞在 YK-ADC 管理端口或 self IP 地址下，执行任意高级 Shell（bash）命令、创建或删除文件，甚至绕过设备模式的安全限制。	CVE-2025-59481	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC IPsec 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 IPsec 模块存在拒绝服务漏洞，该漏洞产生的原因是未公开的特定流量可导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞造成 YK-ADC 系统的拒绝服务，导致流量中断，TMM 进程重启。	CVE-2025-58071	网络设备（交换机、路由器等网络端设备）	YK-ADC###YK-ADC Next CNF###YK-ADC Next for Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC iRules HTTP::respond 命令拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 iRules 模块存在拒绝服务漏洞，该漏洞产生的原因是 iRule 中配置了 HTTP::respond 命令时，未公开的请求会导致内存资源利用率增加。攻击者可利用该漏洞造成拒绝服务。	CVE-2025-46706	网络设备（交换机、路由器等网络端设备）	YK-ADC###YK-ADC NextSPK###YK-ADC NextCNF	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC iRules ILX::call 命令拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 iRules 模块存在拒绝服务漏洞，该漏洞产生的原因是当 iRule 使用 ILX::call 命令并配置在虚拟服务器上时，未公开的流量可能导致 Traffic Management Microkernel（TMM）进程终止。攻击者可利用该漏洞导致 YK-ADC 系统发生拒绝服务。	CVE-2025-53474	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC 产品 MPTCP 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 MPTCP 模块存在拒绝服务漏洞，该漏洞产生的原因是当在虚拟服务器上配置启用 MPTCP 的 TCP 配置文件时，特定未公开的流量与攻击者无法控制的条件共同作用，会导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞造成 YK-ADC 系统的拒绝服务。	CVE-2025-48008	网络设备（交换机、路由器等网络端设备）	YK-ADC#YK-ADC Next SPK#YK-ADC Next CNF	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科公司 YK-ADC Next 产品拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC Next CNF、SPK 及 Kubernetes 存在拒绝服务漏洞，该漏洞产生的原因是重复的未公开 API 调用会导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞触发拒绝服务。	CVE-2025-55670	网络设备（交换机、路由器等网络端设备）	YK-ADC Next SPK#### YK-ADC Next CNF#### #YK-ADC Next for Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科公司 YK-ADC Next CNF、SPK 及 Kubernetes 产品拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC Next 的 HTTP/2 Ingress 模块存在拒绝服务漏洞，该漏洞产生的原因是未公开的流量可导致流量管理微内核（TMM）进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-58120	网络设备（交换机、路由器等网络端设备）	YK-ADC Next SPK#### YK-ADC Next CNF#### YK-ADC Next for Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科公司 YK-ADC PEM 模块拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC PEM 模块存在拒绝服务漏洞。该漏洞产生的原因是在虚拟服务器配置了分类配置文件但未配置 HTTP 或 HTTP/2 配置文件时，未公开的请求可能导致流量管理微内核（TMM）终止。攻击者可利用该漏洞导致 YK-ADC 系统发生拒绝服务。	CVE-2025-54479	网络设备（交换机、路由器等网络端设备）	YK-ADC##YK-ADC Next CNF###YK-ADC Next for Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科公司 YK-ADC SCP 和 SFTP 权限绕过漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 SCP 和 SFTP 模块存在权限绕过漏洞，该漏洞产生的原因是攻击者可通过未公开的命令绕过 Appliance 模式的限制。攻击者可利用该漏洞在 Appliance 模式下绕过安全限制，获取本不应有的操作权限。	CVE-2025-53868	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC SSL Orchestrator 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 SSL Orchestrator 模块存在拒绝服务漏洞，该漏洞产生的原因是启用 SSL Orchestrator 后，未公开的流量可能导致 Traffic Management Microkernel（TMM）进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-41430	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC SSL Orchestrator 内存损坏漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC SSL Orchestrator 的显式前向代理模块存在内存损坏漏洞，该漏洞产生的原因是当在虚拟服务器上配置显式前向代理并启用代理连接功能时，未公开的流量可能导致内存损坏。攻击者可利用该漏洞导致系统性能下降，最终可能导致 Traffic Management Microkernel（TMM）进程被强制重启或手动重启，造成拒绝服务（DoS）。	CVE-2025-55036	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC SSL/TLS 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 SSL/TLS 模块存在拒绝服务漏洞。该漏洞产生的原因是在配置了 Diffie-Hellman(DH)组椭圆曲线密码学(ECC)Brainpool 曲线，并将该 SSL 配置文件应用于虚拟服务器时，未公开的流量可导致流量管理微内核(TMM)进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击。	CVE-2025-60016	网络设备（交换机、路由器等网络端设备）	YK-ADC###YK-ADC NextSPK###YK-ADC NextCNF	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC TMM 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 TMM（Traffic Management Microkernel）模块存在拒绝服务漏洞，该漏洞产生的原因是当数据库变量 tm.tcpudptxchecksum 被配置为非默认值 Software-only 时，特定的未公开流量可能导致 TMM 进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务（DoS）攻击。	CVE-2025-58096	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC TMM 数据篡改漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 TMM 模块存在数据篡改漏洞，该漏洞产生的原因是未公开的流量可导致在缺乏消息完整性保护的协议中发生数据损坏和未经授权的数据修改。攻击者可利用该漏洞向未启用消息完整性保护（如未使用 TLS）的活动 TCP 连接注入恶意数据，造成远程未认证的数据篡改。	CVE-2025-58424	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	高

云科 YK-ADC 故障诊断工具权限绕过漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的故障诊断工具存在权限绕过漏洞，该漏洞产生的原因是故障诊断工具未正确限制具有资源管理员角色的认证用户，导致其可以绕过命令限制并获得 Advanced Shell（bash）访问权限。攻击者可利用该漏洞绕过 Appliance 模式下的安全边界，获取更高权限，造成系统安全风险。	CVE-2025-61958	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 OS 越界写入漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为容翼 r 系列硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS 的 SW_DAG 进程模块存在越界写入漏洞，该漏洞产生的原因是内存写入操作未正确限制，导致可能发生内存损坏。攻击者可利用该漏洞通过云科 OS 租户系统发起认证攻击，造成拒绝服务。	CVE-2025-60015	网络设备（交换机、路由器等网络端设备）	云科 OS-Appliance###云科 OS-Chassis	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	本地	低

云科 OS 系统 SNMP 拒绝服务漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为容翼 r 系列硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS 系统的 SNMP 模块存在拒绝服务漏洞，该漏洞产生的原因是 SNMP 配置后，未公开的请求可导致 SNMP 内存资源利用率增加。攻击者可利用该漏洞远程认证后发起攻击，导致系统性能下降，最终可能引发 SNMP 进程重启或系统重启，影响云科 OS 系统的可用性。	CVE-2025-47150	网络设备（交换机、路由器等网络端设备）	云科 OS-Appliance###云科 OS-Chassis	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 OS 本地权限提升漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为容翼 r 系列硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS 系统存在本地权限提升漏洞，该漏洞产生的原因是认证攻击者可通过本地访问绕过 Appliance 模式安全机制，执行具有更高权限的系统命令。攻击者可利用该漏洞跨越安全边界，获取更高系统权限，造成系统安全风险。	CVE-2025-57780	网络设备（交换机、路由器等网络端设备）	云科 OS - Appliance ### 云科 OS - Chassis	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	本地	低

云科 OS 系统云科 OS-A 和云科 OS-C 模块本地权限提升漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为容翼 r 系列硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS 系统的云科 OS-A 和云科 OS-C 模块存在本地权限提升漏洞，该漏洞产生的原因是认证攻击者可通过本地访问绕过 Appliance 模式安全机制，执行任意系统命令以获取更高权限。攻击者可利用该漏洞跨越安全边界，造成系统权限被非法提升。	CVE-2025-61955	网络设备（交换机、路由器等网络端设备）	云科 OS-Appliance### 云科 OS-Chassis	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	本地	低

云科 云科 OS-A 产品 FIPS 模块命令注入漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为 r 系列和 VELOS 硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS-A 产品的 FIPS 硬件安全模块（HSM）存在命令注入漏洞，该漏洞产生的原因是初始化 FIPS 模块时，使用包含特殊 shell 元字符的密码，导致模块未正确初始化。攻击者可利用该漏洞在初始化 FIPS HSM 时执行任意系统命令，可能创建或删除文件、禁用服务或绕过 Appliance 模式。该漏洞仅影响搭载 FIPS HSM 的 rSeries 硬件 r5920-DF 和 r10920-DF。	CVE-2025-60013	网络设备（交换机、路由器等网络端设备）	云科 OS - Appliance	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	本地	低

云科 云科 OS-A 软件 FIPS HSM 信息泄露漏洞	云科 OS 是云科公司推出的新一代网络操作系统，专为容翼 r 系列硬件平台设计，提供模块化、可编程和多租户的现代化网络服务管理平台。 云科 OS-A 软件的 FIPS 硬件安全模块（HSM）存在信息泄露漏洞，该漏洞产生的原因是攻击者可在短时间窗口内读取进程信息，导致敏感 FIPS HSM 信息暴露。攻击者可利用该漏洞在云科 rSeries r5920-DF（C136）和 r10920-DF（C137）设备访问敏感 FIPS HSM 信息。	CVE-2025-53860	网络设备（交换机、路由器等网络端设备）	云科 OS-Appliance	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	本地	高

云科 YK-ADC ePVA 拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 ePVA 模块存在拒绝服务漏洞，该漏洞产生的原因是当虚拟服务器、NAT 对象或 SNAT 对象使用 ePVA 功能且 Auto LastHop 设置被禁用时，未公开的流量可能导致 TMM 进程终止。攻击者可利用该漏洞造成 YK-ADC 系统的拒绝服务。	CVE-2025-53856	网络设备（交换机、路由器等网络端设备）	YK-ADC	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC Next TMM 内存资源管理漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC Next 的 TMM 模块存在内存资源管理漏洞，该漏洞产生的原因是在通过声明式 API 在虚拟服务器上配置 iRule 后，重新实例化时清理过程会导致 TMM 内存资源利用率增加。攻击者可利用该漏洞导致系统性能下降，最终可能引发拒绝服务。	CVE-2025-54805	网络设备（交换机、路由器等网络端设备）	YK-ADC Next SPK#### YK-ADC Next CNF#### #YK-ADC Next for Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC SSL/TLS 配置文件拒绝服务漏洞	云科 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 的 SSL/TLS 模块存在拒绝服务漏洞，该漏洞产生的原因是当在虚拟服务器上配置客户端 SSL 配置文件时，未公开的请求会导致内存资源利用率增加。攻击者可利用该漏洞导致系统性能下降，最终可能造成拒绝服务影响。	CVE-2025-61974	网络设备（交换机、路由器等网络端设备）	YK-ADC###YK-ADC NextSPK####YK-ADC NextCNF####YK-ADC Nextfor Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低

云科 YK-ADC TMM 模块拒绝服务漏洞	5 YK-ADC 是云科公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。 YK-ADC 系统的 TMM 模块存在拒绝服务漏洞，该漏洞产生的原因是多板卡平台在有多于一个板卡时，未公开的流量可能导致 TMM 进程终止。攻击者可利用该漏洞对 YK-ADC 系统发起拒绝服务攻击，造成流量中断并导致 TMM 进程重启。	CVE-2025-61990	网络设备（交换机、路由器等网络端设备）	YK-ADC##YK-ADC NextSPK####YK-ADC NextCNF####YK-ADC Nextfor Kubernetes	17.5.1.3,17.1.3	2025/10/15	修复版本正在做稳定性测试，新版本镜像 10 月 24 号正式发布，获取热线电话：4006160001	远程网络	低