K000137053：神州云科漏洞概述（2023 年 10 月）

发布日期：2023 年 10 月 10 日

安全顾问描述

注意：神州云科致力于快速响应神州云科产品中的潜在漏洞。与所有公开已知的漏洞一样，神州云科致力于在彻底调查漏洞后立即发布响应。在这种情况下，一名外部研究人员通知神州云科，他们的发现将于 10 月 10 日公开。为了减少对买家的影响，我们决定将 10 月 18 日的 QSN 推迟到 10 月 10 日，以减轻多次披露造成的中断。

2023 年 10 月 10 日，神州云科宣布了以下安全问题。本文档旨在概述这些漏洞和安全风险，以帮助确定对 神州云科设备的影响。您可以在相关文章中找到每个问题的详细信息。

- 高 CVE
- 中型 CVE
- 安全风险

高 CVE

文章 （CVE）	CVSS 评分	受影响的产品	受影响的版本	引入的修复
K000135689：YK-ADC 配置实用程序漏洞 CVE-2023-413	8.8 – 标准部署 9.9 – 设备模式	YK-ADC （所有模块）	17.1.0 15.1.0 – 15.1.10 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0.2 15.1.10.2 14.1.5.6

73				
K41072952： YK-ADC 设备模式外部监控器漏洞 CVE-2023-43746	8.7 – 仅限设备模式	YK-ADC（所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
K29141800：多刀片 VIPRION 配置实用程序会话 Cookie 漏洞 CVE-2023-40537	8.1	YK-ADC（所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
K000136185：适用于 macOS 的 YK-ADC Edge Client 漏洞 CVE-2023-43611	7.8	大 IP（APM）	17.1.0 15.1.0 – 15.1.10 14.1.0 – 14.1.5 13.1.0 – 13.1.5	没有
		APM 客户端	7.2.3 – 7.2.4	7.2.4.4

K000133467： YK-ADC HTTP/2 漏洞 CVE-2023-40534	7.5	YK-ADC （所有模块）	17.1.0 – 17.1.1	17.1.1.1 17.1.1 + 修补程序 -BIGIP-17.1.1.0.2.6-ENG2 17.1.0.3 + 修补程序 -BIGIP-17.1.0.3.0.23.4-ENG2 + 修补程序 -BIGIP-.0.13.5-ENG2
		YK-ADC Next SPK	1.6.0 – 1.8.2	没有
K000134652： YK-ADC TCP 配置文件漏洞 CVE-2023-40542	7.5	YK-ADC （所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
K000132420： YK-ADC IPsec 漏洞 CVE-2023-41085	7.5	YK-ADC （所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9

K000135874：YK-ADC Next SPK SSH 漏洞 CVE-2023-45226	7.4	YK-ADC Next SPK	1.5.0	1.6.0
K000135040：适用于 macOS 的 YK-ADC Edge 客户端漏洞 CVE-2023-5450	7.3	大 IP（APM）	17.1.0 15.1.0-15.1.10 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.1.1 15.1.10.3
		APM 客户端	7.2.3 – 7.2.4	7.2.4.5
K26910459：YK-ADC iControl REST 漏洞 CVE-2023-42768	7.2	YK-ADC（所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9

[1]神州云科仅评估尚未达到其生命周期的技术支持结束（EoTS）阶段的软件版本。

[2]神州云科已在工程修补程序中修复了此问题，该修补程序可用于尚未达到软件开发结束的 YK-ADC 系统版本。受此问题影响的可以从神州云科下载页面下

载工程修补程序。有关更多信息，请参阅 K000090258：从神州云科下载神州云科产品。虽然神州云科努力发布尽可能稳定的代码，但工程修补程序并未对计划软件版本进行广泛的 QA 评估。神州云科提供工程修补程序，不提供任何可用性保证或保证。有关修补程序策略的更多信息，请参阅 K4918：神州云科严重问题修补程序策略概述。

中型 CVE

文章 （CVE）	CVSS 评分	受影响的产品	受影响的版本 [1]	引入的修复
K98334513：YK-ADC DNS TSIG 关键漏洞 CVE-2023-41253	5.5	YK-ADC （DNS、LTM 通过 DNS 服务许可证启用）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
K06110200：YK-ADC 和 BIG-IQ TACACS+ 审核日志漏洞 CVE-2023-43485	5.5	YK-ADC（所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
		BIG-IQ 集中管理	8.0.0 – 8.3.0	8.3.0 + 修补程序 -BIG-IQ-8.3.0.0.12.118-ENG [2] 8.2.0.1 + 修补程序

				-BIG-IQ-8.2.0.1.0.1 3.97-ENG2
K000137106： HTTP/2 漏洞 CVE-2023-44 487	5.3	YK-ADC Next （所有模块）	20.0.1 – 20.0.2	20.1.0
		YK-ADC Next SPK	1.5.0 – 1.8.2	没有
		YK-ADC（所 有模块）	17.1.0 – 17.1.1 15.1.0 – 15.1.10 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.1.3 15.1.10.4
		NGINX 加	R25 – R30	R30 P1 R29 P1
		NGINX OSS	1.9.5 – 1.25.2	没有
		NGINX Ingress 控制器	3.0.0 – 3.3.0 2.0.0 – 2.4.2 1.12.2 – 1.12.5	没有
K20307245： YK-ADC tmsh 漏洞 CVE-2023-45 219	4.4	YK-ADC（所 有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9

K47756555： YK-ADC APM 引导式配置漏洞 CVE-2023-39447	4.4	大 IP （APM）	15.1.0 – 15.1.7	17.1.0 15.1.8
		YK-ADC（引导式配置）	8.0 7.0 – 7.7 6.0	9.0
K20850144： YK-ADC 和 BIG-IQ DB 变量漏洞 CVE-2023-41964	4.3	YK-ADC（所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
		BIG-IQ 集中管理	8.0.0 – 8.3.0	8.3.0 + 修补程序 -BIG-IQ-8.3.0.0.12.118-ENG[2] 8.2.0.1 + 修补程序 -BIG-IQ-8.2.0.1.0.13.97-ENG[2]

[1] 神州云科仅评估尚未达到其生命周期的技术支持结束 （EoTS） 阶段的软件版本。

[2] 神州云科已在工程修补程序中修复了此问题，该修补程序可用于尚未达到软件开发结束的 BIG-IQ 系统版本。受此问题影响的可以从 神州云科下载页面下载工程修补程序。有关更多信息，请参阅 K000090258：从神州云科下载神州云科产品。虽然神州云科努力发布尽可能稳定的代码，但工程修补程序并未对计划软

件版本进行广泛的 QA 评估。神州云科提供工程修补程序，不提供任何可用性保证或保证。有关修补程序策略的更多信息，请参阅 K4918：神州云科严重问题修补程序策略概述。

安全风险

文章 （曝光）	受影响的产品	受影响的版本 [1]	引入的修复
K75431121：带 SSO 的 YK-ADC APM OAuth 持有者无法按预期处理 HTTP 标头	大 IP （APM）	15.1.0 – 15.1.8 14.1.0 – 14.1.5	17.1.0 15.1.9
K21800102：将重定向 iRule 应用于虚拟服务器时，将绕过 HTTP RFC 强制实施	YK-ADC(所有模块）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
K000135944：攻击签名检查安全风险	YK-ADC（高级 WAF/ASM）	15.1.0 – 15.1.8 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 15.1.9
	NGINX App Protect WAF	4.0.0 – 4.1.0 3.3.0 – 3.12.2	4.2.0

[1] 神州云科仅评估尚未达到其生命周期的技术支持结束 （EoTS） 阶段的软件版本。