K000138353：季度安全通知（2024 年 2 月）

发布日期：2024 年 2 月 14 日更新日期：2024 年 2 月 14 日

安全顾问描述

2024 年 2 月 14 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
- 低 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
K000137522：YK-ADC iControl REST 漏洞 CVE-2024-22093	8.7	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9
K000134516：YK-ADC SSL 客户端证书 LDAP 和 CRLDP 身份验证配置文件漏洞 CVE-2024-23979	7.5	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9
K000135873：YK-ADC Websockets 漏洞	7.5	YK-ADC（高级 WAF/ASM）	15.1.0–15.1.8	17.1.0

CVE-2024-21849				
K000135946：YK-ADC PEM 漏洞 CVE-2024-23982	7.5	大 IP （PEM）	17.1.0 – 17.1.1[2] 15.1.0–15.1.10[2]	没有[2]
K000137270：YK-ADC Advanced WAF 和 YK-ADC ASM 漏洞 CVE-2024-21789	7.5	YK-ADC（高级 WAF/ASM）	17.1.0	17.1.1
K000137333：YK-ADC TMM 漏洞 CVE-2024-24775	7.5	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.9	17.1.1 15.1.10
K000137334：神州云科应用可见性和报告模块以及 YK-ADC 高级 WAF/ASM 漏洞 CVE-2024-23805	7.5	应用可见性和报告模块和 YK-ADC（高级 WAF/ASM）	17.1.0 15.1.0 – 15.1.9	17.1.1 15.1.10
K000137416：YK-ADC Advanced WAF 和 YK-ADC ASM 漏洞 CVE-2024-23308	7.5	YK-ADC（高级 WAF/ASM）	17.1.0	17.1.1
K000137521：YK-ADC	7.5	大 IP （AFM）	17.1.0	17.1.1

AFM 漏洞 CVE-2024-21763			15.1.0 – 15.1.9	15.1.10
K000137595：YK-ADC AFM 签名匹配漏洞 CVE-2024-21771	7.5	大 IP （AFM + IPS）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9
K000137675：YK-ADC HTTP/2 漏洞 CVE-2024-23314	7.5	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9
		YK-ADC Next SPK	1.5.0 – 1.8.0	1.8.1
K000138444：NGINX HTTP/3 QUIC 漏洞 CVE-2024-24989	7.5	NGINX 加	R31 系列	R31 P1
		NGINX 开源	1.25.3	1.25.4
K000138445：NGINX HTTP/3 QUIC 漏洞 CVE-2024-24990	7.5	NGINX 加	R30 – R31	R31 P1 R30 P2
		NGINX 开源	1.25.0 – 1.25.3	1.25.4
K32544615：YK-ADC iControl REST API 漏洞 CVE-2024-22389	7.2	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 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]任何 YK-ADC ISO 文件中包含的分类签名均不受此问题的影响。易受攻击的分类签名可在 2022 年 9 月 8 日至 2023 年 2 月 16 日期间在神州云科上下载。如果您在此期间手动更新了签名文件，则您的系统可能正在运行易受攻击的版本。此外，如果您在此期间在 YK-ADC PEM 系统上启用了自动下载，则您的系统可能正在运行易受攻击的版本。有关受影响和已修复特征码的列表，以及要确定您的系统正在运行的特征码，请参阅文章。

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
K98606833：YK-ADC 和 BIG-IQ SCP 漏洞 CVE-2024-21782	6.7	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9
		BIG-IQ 集中式管理器	8.0.0 – 8.3.0	8.3.0 + 修补程序 BIG-IQ-8.3.0.0.16.118-ENG[2]
K000133111：YKOS 漏洞 CVE-2024-24966	6.2	YKOS-A 系列	1.2.0	1.3.0
		YKOS-C 系列	1.3.0 – 1.5.1	1.6.0
K91054692：YK-ADC 设	6.0	YK-ADC（所有模块）	17.1.0 15.1.0 – 15.1.8	17.1.1 15.1.9

备模式 iAppsLX 漏洞 CVE-2024-23 976				
K000132800： YKOS QKView 实用程序漏洞 CVE-2024-23 607	5.5	YKOS-A 系列	1.3.0 – 1.3.2	1.4.0
		YKOS-C 系列	1.3.0 – 1.5.1	1.6.0
K000137886： YK-ADC Next CNF 漏洞 CVE-2024-23 306	4.4	YK-ADC Next CNF	1.1.0 – 1.1.1	1.2.0

[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。

[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。

低 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
K000138047：YK-ADC Advanced WAF 和 YK-ADC ASM 配置实用程序漏洞 CVE-2024-23603	3.8	YK-ADC（高级 WAF/ASM）	17.1.0 15.1.0 – 15.1.9	17.1.1 15.1.10

[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。

安全风险

文章 （CVE）	受影响的产品	受影响的版本 [1]	引入的修复
K11453402：YK-ADC Cookie 加密安全风险	YK-ADC Next SPK	1.5.0 – 1.8.0	1.8.2
	YK-ADC Next CNF	1.1.0 – 1.1.1	1.2.0
	YK-ADC（所有模块）	15.1.0 – 15.1.8	17.1.0 15.1.9

K000137796：YK-ADC SSL 配置文件安全风险	YK-ADC（所有模块）	17.1.0 15.1.0 -15.1.10	17.1.1.2 15.1.10.3

[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。