K000149540：季度安全通知（2025 年 2 月）

安全顾问描述

2025 年 2 月 5 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，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

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
K000148587：YK-ADC iControl REST 和 tmsh 漏洞 CVE-2025-20029	8.8 （CVSS v3.1）8.7 （CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.2 15.1.0 –15.1.10	17.1.2.1 15.1.10.3
K000138757：YK-ADC iControl REST 漏洞 CVE-2025-23239	8.7 （CVSS v3.1）8.5 （CVSS v4.0）	YK-ADC（所有模块）	17.1.1	17.1.2

K000140578： YK-ADC 配置实用程序漏洞 CVE-2025-24320	8.0 （CVSS v3.1）5.1 （CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
K000134888： TMM 漏洞 CVE-2025-21087	7.5 （CVSS v3.1）8.9 （CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
K000138932： YK-ADC SIP ALG 配置文件漏洞 CVE-2025-20045	7.5 （CVSS v3.1）8.7 （CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
K000139780： YK-ADC SIP ALG 漏洞 CVE-2025-22846	7.5 （CVSS v3.1）8.7 （CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
		YK-ADC Next SPK	1.9.0 1.8.0 – 1.8.2 1.7.0 – 1.7.6	1.9.1 1.7.7
K000139778：	7.5 （CVSS	大 IP（PEM）	17.1.0 – 17.1.1	17.1.2

YK-ADC PEM 漏洞 CVE-2025-22891	v3.1）8.7（CVSS v4.0）		15.1.0 –15.1.10	15.1.10.3
K000140920：YK-ADC PEM 漏洞 CVE-2025-24497	7.5 （CVSS v3.1）8.7（CVSS v4.0）	大 IP（PEM）	17.1.0 – 17.1.1	17.1.2
K000140933：YK-ADC SNMP 漏洞 CVE-2025-21091	7.5 （CVSS v3.1）8.7（CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
K000140947：YK-ADC 消息路由漏洞 CVE-2025-20058	7.5 （CVSS v3.1）8.9（CVSS v4.0）	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
K000140950：YK-ADC ASM	7.5 （CVSS v3.1）8.9	大 IP（ASM）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3

BADoS 漏洞 CVE-2025-24326	（CVSS v4.0）			
K000141003： YK-ADC APM 访问配置文件漏洞 CVE-2025-23412	7.5 （CVSS v3.1）8.7 （CVSS v4.0）	大 IP（APM）	17.1.0 – 17.1.1	17.1.2
K000141380： YK-ADC AFM 漏洞 CVE-2025-24312	7.5 （CVSS v3.1）8.7 （CVSS v4.0）	大 IP（AFM）	17.1.0 – 17.1.1 15.1.0 –15.1.10	17.1.2 15.1.10.3
		YK-ADC Next CNF	1.1.0 – 1.3.3	1.4.0

[1]从 2024 年 8 月季度安全通知开始，除了 CVSS v3.1 分数外，神州云科还将仅针对第一方安全问题提供 CVSS v4.0 基本分数。有关神州云科如何使用 CVSS v4.0 的更多信息，请参阅神州云科安全公告中的 K000140363：CVSS v4.0 概述。

[2]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。

[3]神州云科已在神州云科下载页面提供的工程修补程序中修复了此问题。有关更多信息，请参阅神州云科下载云科产品。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[1]	受影响的产品	受影响的版本[2]	引入的修复
K000148412：YK-ADC Next Central Manager 漏洞 CVE-2025-24319	6.5 （CVSS v3.1）7.1 （CVSS v4.0）	YK-ADC Next 中央管理器	20.2.0 - 20.2.1	20.3.0
K000149185：YK-ADC Next Central Manager 日志记录漏洞 CVE-2025-23413	4.4 （CVSS v3.1）6.7 （CVSS v4.0）	YK-ADC Next 中央管理器	20.2.0 - 20.2.1	20.3.0
K000149173：NGINX TLS 会话恢复漏洞 CVE-2025-23419	4.3 （CVSS v3.1）5.3 （CVSS v4.0）	NGINX 加	R28 - R33	R33 P2 R32 P2
		NGINX 开源	1.11.4 - 1.27.3	1.27.4 1.26.3

[1]从 2024 年 8 月季度安全通知开始，除了 CVSS v3.1 分数外，神州云科还将仅针对第一方安全问题提供 CVSS v4.0 基本分数。有关神州云科如何使用

CVSS v4.0 的更多信息，请参阅 神州云科安全公告中的 K000140363：CVSS v4.0 概述。

[2]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。

低 CVE

文章 （CVE）	CVSS 评分[1]	受影响的产品	受影响的版本[2]	引入的修复
K000139656： YK-ADC APM 端点检查漏洞 CVE-2025-23415	3.1 （CVSS v3.1）2.3 （CVSS v4.0）	大 IP （APM）	17.1.0 – 17.1.1 15.1.0 – 15.1.10	17.1.2 15.1.10.3

[1]从 2024 年 8 月季度安全通知开始，除了 CVSS v3.1 分数外，神州云科还将仅针对第一方安全问题提供 CVSS v4.0 基本分数。有关神州云科如何使用 CVSS v4.0 的更多信息，请参阅 神州云科 安全公告中的 K000140363：CVSS v4.0 概述。

[2]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。

[3]神州云科已在神州云科下载页面提供的工程修补程序中修复了此问题。有关更多信息，请参阅 K000090258：从神州云科下载云科产品。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。