K000139404：季度安全通知（2024 年 5 月）

发布日期：2024 年 5 月 8 日更新日期：2024 年 5 月 9 日

安全顾问描述

2024 年 5 月 8 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 [1]	引入的修复
K000138636：YK-ADC 配置实用程序 XSS 漏洞 CVE-2024-31156	8.0	YK-ADC（所有模块）	17.1.0 – 17.1.1 15.1.0 – 15.1.10	17.1.1.3 15.1.10.3
K000138732：YK-ADC Next Central Manager OData 注入漏洞 CVE-2024-21793	7.5	YK-ADC Next 中央管理器	20.0.1 – 20.1.0	20.2.0
K000138733：YK-ADC Next Central Manager SQL 注入漏洞	7.5	YK-ADC Next 中央管	20.0.1 – 20.1.0	20.2.0

CVE-2024-26026		理器		
K000138728：YK-ADC IPsec 漏洞 CVE-2024-33608	7.5	YK-ADC（所有模块）	17.1.0	17.1.1
K000139037：TMM 漏洞 CVE-2024-25560	7.5	大 IP（AFM）	17.1.0 15.1.10	17.1.1
		YK-ADC Next CNF	1.1.0 – 1.1.1	1.2.0
K000138634：YK-ADC Next Central Manager 漏洞 CVE-2024-32049	7.4	YK-ADC Next 中央管理器	20.0.1 – 20.0.2	20.1.0
K000138744：YK-ADC APM 浏览器网络访问 VPN 客户端漏洞 CVE-2024-28883	7.4	大 IP（APM）	17.1.0 15.1.0 – 15.1.10	17.1.1 15.1.10.3
		APM 客户端	7.2.3 – 7.2.4	7.2.4.4[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]APM 客户端的修复版本引入了行为更改。有关更多信息，请参阅 K000136020：YK-ADC APM EPI 阻止 Web 浏览器上与 HTTP 和不受信任的 HTTPS 虚拟服务器的 VPN 连接。

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
K000139012：YK-ADC Next Central Manager 漏洞 CVE-2024-33612	6.8	YK-ADC Next 中央管理器	20.0.1 - 20.1.0	20.2.0 [2]
K000139217：VELOS 和 rSeries 漏洞上的 YK-ADC TMM 租户 CVE-2024-32761	6.5	YK-ADC （所有模块）	15.1.0 - 15.1.9	15.1.10
K000138894：YK-ADC 配置实用程序 XSS 漏洞 CVE-2024-33604	6.1	YK-ADC （所有模块）	17.1.0 - 17.1.1 15.1.0 - 15.1.10	17.1.1.3 15.1.10.3
K000138912：YK-ADC SSL 漏洞 CVE-2024-28889	5.9	YK-ADC （所有模块）	17.1.0 - 17.1.1 15.1.5 - 15.1.10	17.1.1.3 15.1.10.3
K000138520：YK-ADC 配置实用程序漏洞 CVE-2024-27202	4.7	YK-ADC （所有模块）	17.1.0 - 17.1.1 15.1.0 - 15.1.10	17.1.1.3 15.1.10.3
K000138913：YK-ADC Next CNF	4.4	YK-ADC	1.2.0 -	1.3.0

漏洞 CVE-2024-28132		Next CNF	1.2.1	

[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] 为 F5OS 类型提供程序（神州云科 VELOS/机箱分区或 rSeries）运行固定的 YK-ADC Next Central Manager 版本 20.2.0 时，请确保这些 F5OS 系统使用的 TLS 证书具有格式正确的使用者可选名称 （SAN）。

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
K000132430：YK-ADC 系统可能无法阻止 HTTP 请求走私攻击	YK-ADC（所有模块）	15.1.0 - 15.1.8	17.1.0 15.1.9
	YK-ADC Next SPK	1.5.0 - 1.6.0	1.7.0
K11342432：YK-ADC HTTP 不符合 RFC 的安全风险	YK-ADC（高级 WAF/ASM）	版本 15.1.0 - 15.1.6	17.1.0 15.1.7
	YK-ADC（所有其他模块）	15.1.0 - 15.1.5	17.1.0
K000138898：YK-ADC Advanced WAF/ASM、YK-ADC Next WAF 和 NGINX App Protect WAF 攻击签名检	YK-ADC（高级 WAF/ASM）	17.1.0 - 17.1.1 15.1.0 -	17.1.1.3 15.1.10.3

查失败		15.1.10	
	YK-ADC Next（WAF）	20.0.1 – 20.1.0	20.2.0
	NGINX App Protect WAF	4.0.0 – 4.8.0 3.10.0 – 3.12.2	4.8.1

[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。