K30425568：神州云科漏洞概述（2022 年 10 月）

发布日期：2022 年 10 月 19 日更新日期：2023 年 12 月 6 日

安全顾问描述

2022 年 10 月 19 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。您可以在关联的安全通告中找到每个问题的详细信息。

分布式云和托管服务

服务	地位
神州云科分布式云服务	不影响或已解决
银线	不影响或已解决
威胁堆栈	不影响或已解决

- 高 CVE
- 中型 CVE
- 低 CVE
- 安全风险

高 CVE

安全公告 （CVE）	CVSS 评分	受影响的产品	受影响的版本	引入的修复
K33484483：F5OS 漏洞 CVE-2022-41835	8.8	F5OS-A 系列	1.0.0 - 1.0.1	1.1.0
		F5OS-C 系列	1.3.0 - 1.3.2	1.5.0
K43024307：YK-ADC iRules 漏洞	7.5	YK-ADC（所有模块）	17.0.0 15.1.0 - 15.1.6	17.1.0 17.0.0.1

CVE-2022-41624			14.1.0 – 14.1.5 13.1.0 – 13.1.5	15.1.7 14.1.5.2 13.1.5.1
K02694732：YK-ADC Advanced WAF 和 ASM bd 漏洞 CVE-2022-41691	7.5	YK-ADC（高级 WAF、ASM）	14.1.5	14.1.5.2
K70569537：YK-ADC DNS Express 漏洞 CVE-2022-41787	7.5	YK-ADC（DNS、LTM 通过 DNS 服务许可证启用）	17.0.0 15.1.0 – 15.1.6 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 17.0.0.1 15.1.6.1 14.1.5.1 13.1.5.1
K00721320：YK-ADC AFM NAT64 策略漏洞 CVE-2022-41806	7.5	大 IP （AFM）	15.1.0 – 15.1.5	17.0.0 15.1.5.1
K10347453：YK-ADC SIP 配置文件漏洞 CVE-2022-41832	7.5	YK-ADC（所有模块）	17.0.0 15.1.0 – 15.1.6 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 17.0.0.1 15.1.6.1 14.1.5.1 13.1.5.1
K69940053：YK-ADC	7.5	YK-ADC（所有	13.1.0 – 13.1.5	14.1.0

iRules 漏洞 CVE-2022-41833		模块）		
K47204506：YK-ADC Advanced WAF 和 ASM bd 漏洞 CVE-2022-41836	7.5	YK-ADC（高级 WAF、ASM）	17.0.0 15.1.0 – 15.1.6	17.1.0 17.0.0.1 15.1.7
K11830089：YK-ADC Advanced WAF 和 ASM iControl REST 漏洞 CVE-2022-41617	7.2 – 标准部署模式 9.1 – 设备模式	YK-ADC（高级 WAF、ASM）	15.1.0 – 15.1.6 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.0.0 15.1.6.1 14.1.5.1 13.1.5.1
K28112382：NGINX ngx_http_mp4_module 漏洞 CVE-2022-41742	7.1	NGINX 加	R22 – R27	R27 P1 R26 P1
		NGINX 开源订阅	R1 – R2	R2 P1 R1 P1
		NGINX 开源	1.23.0 – 1.23.1 1.1.3 – 1.22.0	1.23.2 1.22.1
		NGINX Ingress 控制器	2.0.0 – 2.4.0 1.9.0 – 1.12.4	2.4.1 1.12.5
K81926432：NGINX ngx_http_mp4_module 漏洞 CVE-2022-41741	7.0	NGINX 加	R22 – R27	R27 P1 R26 P1
		NGINX 开源	R1 – R2	R2 P1

		订阅		R1 P1
		NGINX 开源	1.23.0 – 1.23.1 1.1.3 – 1.22.0	1.23.2 1.22.1
		NGINX Ingress 控制器	2.0.0 – 2.4.0 1.9.0 – 1.12.4	2.4.1 1.12.5
K01112063：NGINX ngx_http_hls_module 漏洞 CVE-2022-41743	7.0	NGINX 加	R22 – R27	R27 P1 R26 P1
		NGINX Ingress 控制器	2.0.0 – 2.4.0 1.9.0 – 1.12.4	2.4.1 1.12.5

[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。

中型 CVE

安全公告 （CVE）	CVSS 评分	受影响的产品	受影响的版本 [1]	引入的修复
K22505850：YK-ADC 和 BIG-IQ iControl REST 漏洞 CVE-2022-41770	6.5	YK-ADC（所有模块）	17.0.0 15.1.0 – 15.1.6 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.1.0 17.0.0.1 15.1.7 14.1.5.1
		BIG-IQ 集中管理	8.0.0 – 8.2.0 7.1.0	没有
K93723284：YK-ADC	6.5	YK-ADC	15.1.0 – 15.1.6	17.0.0

PEM 和 AFM TMUI、TMSH 和 iControl REST 漏洞 CVE-2022-41813		（AFM、PEM）	14.1.0 – 14.1.4 13.1.0 – 13.1.5	15.1.6.1 14.1.5
K81701735：F5OS CLI 漏洞 CVE-2022-41780	5.5	F5OS-A 系列	1.0.0 – 1.0.1	1.1.0
		F5OS-C 系列	1.1.0 – 1.3.2	1.4.0
K52494562：YK-ADC 软件 SYN Cookie 漏洞 CVE-2022-36795	5.3	YK-ADC（所有模块）	17.0.0 15.1.0 – 15.1.6 14.1.0 – 14.1.5	17.1.0 17.0.0.1 15.1.7 14.1.5.1
K64829234：YK-ADC 和 BIG-IQ mcpd 漏洞 CVE-2022-41694	4.9	YK-ADC（所有模块）	15.1.0 – 15.1.6 14.1.0 – 14.1.4 13.1.0 – 13.1.5	17.0.0 15.1.6.1 14.1.5
		BIG-IQ 集中管理	8.0.0 – 8.2.0 7.1.0	8.2.0.1

[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。*

低 CVE

安全公告（CVE）	CVSS 评分	受影响的产品	受影响的版本[1]	引入的修复
K31523465：YK-ADC TMM 漏洞 CVE-2022-41983	3.7	YK-ADC（所有模块）	15.1.0 – 15.1.6 14.1.0 – 14.1.5 13.1.0 – 13.1.5	17.0.0 15.1.7 14.1.5.1

[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。

安全风险

安全建议 （Exposure）	受影响的产品	受影响的版本 [1]	引入的修复
K49237345：YK-ADC Advanced WAF、ASM 和 NGINX App Protect WAF XML 编码安全风险	YK-ADC（高级 WAF、ASM）	15.1.0 – 15.1.5 14.1.0 – 14.1.4 13.1.0 – 13.1.4	17.0.0 15.1.5.1 14.1.4.6 13.1.5
	NGINX App Protect WAF	3.0.0 – 3.11.0 2.0.0 – 2.3.0	3.12.0

[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。