F5 发布 2025 年 2 月季度安全通告

2025-02-08 09:28:33

安全公告编号:CNTA-2025-0002

2 月 5 日，F5 发布了 2025 年第 1 季度的季度安全通告，修复了多款产品存在的 17 个安全漏洞。受影响的产品包括：BIG-IP（14 个）、BIG-IP Next（2 个）、NGINX（1 个）等。

利用上述漏洞，攻击者可进行拒绝服务攻击，或数据泄漏等攻击。CNVD 提醒广大 F5 用户尽快更新至最新版本系统，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高风险等级和风险类型	受影响产品	修复版本
CVE-2025-20029	BIG-IP iControl REST 和 tmsh 漏洞 CVE-2025-20029	高 8.8 数据泄露	BIG-IP	17.1.2.1 16.1.5.2 15.1.10.6
CVE-2025-23239	BIG-IP iControl REST 漏洞 CVE-2025-23239	高 8.7 数据泄露	BIG-IP	17.1.2
CVE-2025-24320	BIG-IP 配置实用程序漏洞 CVE-2025-24320	高 8 数据泄露	BIG-IP	17.1.2 16.1.5.2 15.1.10.6
CVE-2025-21087	TMM 漏洞 CVE-2025-21087	高 7.5 拒绝服务	BIG-IP	17.1.2 Hotfix-BIGIP-16.1.5.2.0.7.5-ENG Hotfix-BIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-21091	BIG-IP SNMP 漏洞 CVE-2025-21091	高 7.5 拒绝服务	BIG-IP	17.1.2 Hotfix-BIGIP-16.1.5.2.0.7.5-ENG Hotfix-BIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-20058	BIG-IP 消息路由漏洞 CVE-2025-20058	高 7.5 拒绝服务	BIG-IP	17.1.2 Hotfix-BIGIP-16.1.5.2.0.7.5-ENG Hotfix-BIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-22891	BIG-IP PEM 漏洞 CVE-2025-22891	高 7.5	BIG-IP	17.1.2 16.1.5

		拒绝服务		HotfixBIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-20045	BIG-IP SIP MRF 漏洞 CVE-2025-20045	高 7.5 拒绝服务	BIG-IP	17.1.2 16.1.5 HotfixBIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-24326	BIG-IP Advanced WAF/ASM BADoS 漏洞 CVE-2025-24326	高 7.5 拒绝服务	BIG-IP	17.1.2 16.1.5 HotfixBIGIP-15.1.10.6.0.11.6-ENG
CVE-2025-23412	BIG-IP APM 访问配置文件漏洞 CVE-2025-23412	高 7.5 拒绝服务	BIG-IP	16.1.5
CVE-2025-22846	BIG-IP SIP 漏洞 CVE-2025-22846	高 7.5 拒绝服务	BIG-IP BIG-IP Next SPK	BIG-IP: 17.1.2 16.1.5 Hotfix-BIGIP-15.1.10.6.0.11.6-ENG BIG-IP Next SPK: 1.9.1 1.7.7
CVE-2025-24312	BIG-IP AFM 漏洞 CVE-2025-24312	高 7.5 拒绝服务	BIG-IP BIG-IP Next CNF	BIG-IP: 17.1.2 Hotfix-BIGIP-16.1.5.2.0.7.5-ENG Hotfix-BIGIP-15.1.10.6.0.11.6-ENG BIG-IP Next CNF: 1.4.0
CVE-2025-24497	BIG-IP PEM 漏洞 CVE-2025-24497	高 7.5 拒绝服务	BIG-IP	17.1.2
CVE-2025-24319	BIG-IP Next Central Manager 漏洞 CVE-2025-24319	中 6.5 拒绝服务	BIG-IP Next Central Manager	BIG-IP Next Central Manager: 20.3.0
CVE-2025-23413	BIG-IP Next Central Manager 漏洞 CVE-2025-23413	中 4.4 数据泄露	BIG-IP Next Central Manager	BIG-IP Next Central Manager: 20.3.0
CVE-2025-23419	TLS 会话恢复漏洞 CVE-2025-23419	中 4.3 数据泄露	NGINX Open Source NGINX Plus	NGINX Open Source: 1.27.4 NGINX Open Source: 1.26.3 NGINX Plus: R32 P2 NGINX Plus: R33 P2

CVE-2025-23415	BIG-IP APM 端点检查漏洞 CVE-2025-23415	低 3.1 数据泄露	BIG-IP	BIG-IP：17.1.2 BIG-IP：16.1.5 BIG-IP：Hotfix-BIGIP-15.1.10.6.0.11.6-ENG

参考信息：https://my.f5.com/manage/s/article/K000140552

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

在发布漏洞公告信息之前，CNVD 都力争保证每条公告的准确性和可靠性。然而，采纳和实施公告中的建议则完全由用户自己决定，其可能引起的问题和结果也完全由用户承担。是否采纳我们的建议取决于您个人或您企业的决策，您应考虑其内容是否符合您个人或您企业的安全策略和流程。

我们鼓励所有计算机与网络安全研究机构，包括厂商和科研院所，向我们报告贵单位所发现的漏洞信息。我们将对所有漏洞信息进行验证并在 CNCERT/CC 网站和国家信息安全漏洞共享平台（CNVD）公布漏洞信息及指导受影响用户采取措施以避免损失。