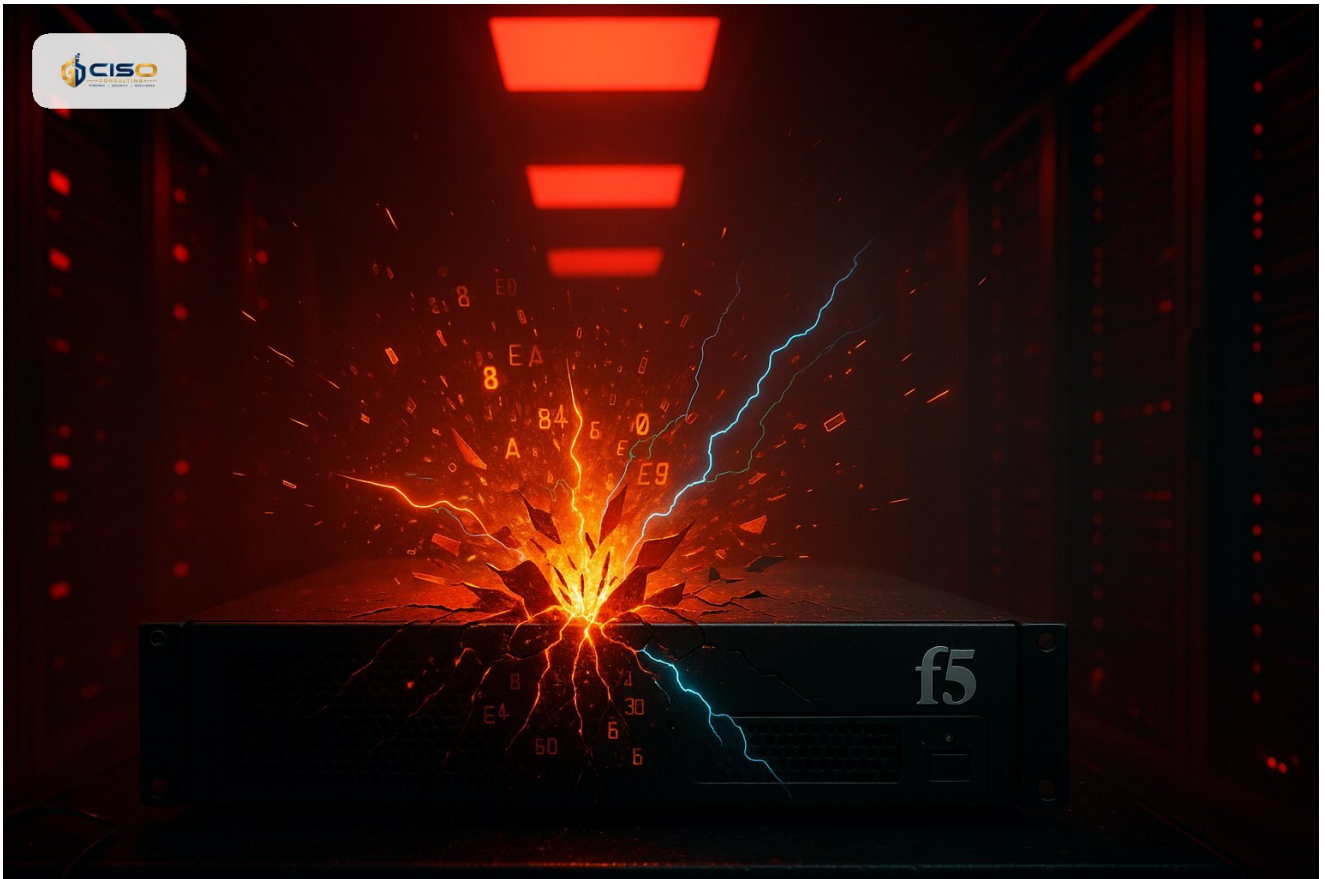


F5 BIG-IP APM Heap Overflow Vulnerability Enables Remote Code Execution



F5 BIG-IP APM contains a heap-based buffer overflow vulnerability allowing unauthenticated remote code execution when access policy and OAuth profile are configured on a virtual server.

- Heap-based buffer overflow vulnerability identified in F5 BIG-IP APM (CVE-2026-94127)
- Unauthenticated attackers can achieve remote code execution on vulnerable systems
- Vulnerability affects systems with access policy and OAuth profile configured on virtual servers
- Vendor mitigations must be applied immediately or affected services discontinued
- Internet-exposed assets require priority assessment and remediation

Vulnerability Overview

F5 Networks has disclosed a **heap-based buffer overflow vulnerability** tracked as CVE-2026-94127 affecting BIG-IP Access Policy Manager (APM). The flaw permits unauthenticated attackers to execute arbitrary code remotely on vulnerable systems. The vulnerability is present when both an access policy and an OAuth profile are configured on a virtual server, a common deployment pattern in enterprise authentication and authorization architectures.

The severity of this vulnerability stems from the combination of remote exploitability without authentication and the potential for complete system compromise through code execution. Organizations using BIG-IP APM for application delivery, access management, or identity federation face immediate risk if systems remain unpatched.

Risk to Saudi Institutions

Regulated institutions in the Kingdom commonly deploy F5 BIG-IP solutions for secure application delivery and access control to critical systems. Financial institutions, healthcare providers, and government entities using BIG-IP APM with OAuth configurations should treat this as a priority incident requiring immediate action. Internet-facing deployments present the highest risk profile and demand urgent attention.

Remediation Guidance

Organizations must apply vendor-supplied mitigations without delay. Where patches or workarounds are unavailable, affected services should be isolated from untrusted networks or discontinued until secure configurations can be implemented. Asset inventories should be reviewed to identify all BIG-IP APM deployments, with particular focus on internet-exposed instances and those handling authentication for sensitive systems. Configuration reviews should verify whether both access policies and OAuth profiles are active on virtual servers.

What to do now

1. Identify all F5 BIG-IP APM deployments across your infrastructure, prioritizing internet-facing instances
2. Verify which systems have both access policy and OAuth profile configured on virtual servers
3. Apply vendor-supplied patches or mitigations immediately in accordance with F5 security advisories
4. Isolate vulnerable systems from untrusted networks or discontinue services if patches are unavailable
5. Review access logs and system activity for indicators of exploitation or unauthorized access attempts
6. Update incident response procedures to include this vulnerability in threat hunting activities