

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

CVE-2026-94127: Critical F5 BIG-IP APM Flaw Under Active Exploitation

Date of Publication

September 23, 2026

Admiralty Code

A1

TA Number

TA2026280

Summary

First Seen: September 22, 2026

Affected Products: F5 BIG-IP Access Policy Manager (APM)

Impact: F5 has disclosed CVE-2026-94127, a critical unauthenticated remote code execution flaw (CVSS 9.8) in the OAuth component of BIG-IP Access Policy Manager (APM), and has confirmed it is being actively exploited in the wild. The flaw is a heap-based buffer overflow that can be triggered with specially crafted traffic. It affects APM versions 21.1.0, 17.5.0 - 17.5.1 and 17.1.0 - 17.1.3, but only on virtual servers where APM acts as an OAuth Authorization Server. Emergency hotfixes are available for all affected branches, and a vendor-supplied iRule mitigation can be used where immediate patching is not possible.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-94127	F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability	F5 BIG-IP Access Policy Manager (APM)			

Vulnerability Details

#1

CVE-2026-94127 is a critical heap-based buffer overflow (CWE-122) in the OAuth component of F5 BIG-IP Access Policy Manager (APM). It allows an unauthenticated remote attacker to execute arbitrary code on affected appliances. The flaw carries a CVSS v3.1 score of 9.8 and a CVSS v4.0 score of 9.3, and the vendor has confirmed active exploitation in the wild at the time of disclosure on September 22, 2026. The vulnerable releases are BIG-IP APM 21.1.0, 17.5.0 through 17.5.1, and 17.1.0 through 17.1.3.

#2

Exposure depends on configuration rather than on the mere presence of APM. Only virtual servers that carry both an APM access policy and an OAuth profile, with APM acting as an OAuth Authorization Server, are vulnerable. Deployments that use APM solely as an OAuth client or resource server are not affected. The flaw resides in the data plane and does not expose the control plane, so restricting access to the management interface offers no protection, and systems running in Appliance mode remain vulnerable. The specific code path responsible for the overflow has not been disclosed.

#3

Exploitation requires only specially crafted traffic sent to an exposed virtual server, with no credentials or user interaction. A successful attack gives the attacker code execution on a perimeter authentication gateway that controls access to downstream applications. No threat actor has been attributed, and no atomic indicators of compromise have been released. Vendor detection guidance instead describes a behavioural sequence: repeated OAuth UserInfo failures with invalid-token errors, followed by suspicious commands in the audit log, and then a Traffic Management Microkernel (TMM) crash.

#4

Emergency hotfixes are available for all three affected branches. Where immediate patching is not possible, an iRule mitigation can be obtained through vendor support to reduce exposure until the hotfix is installed.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-94127	F5 BIG-IP APM (17.1.0 - 17.1.3, 17.5.0 - 17.5.1, 21.1.0)	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*	CWE-122

Recommendations



Apply the Emergency Hotfix Immediately: Install the engineering hotfix that matches the installed BIG-IP APM branch (17.1.x, 17.5.x or 21.x) from F5 Downloads, or move to the corresponding hardened release that already incorporates the fix. Given confirmed exploitation and the absence of any authentication requirement, patching should be treated as an emergency change rather than scheduled into a routine maintenance window.



Preserve Forensic Evidence Before Remediation: Before patching, rebooting or reconfiguring affected appliances, collect and securely retain /var/log/apm, /var/log/audit and any TMM core files so that exploitation can still be assessed afterwards. Remediation activity can overwrite or rotate the very artefacts needed to confirm whether a device was compromised.



Identify Exposed OAuth Authorization Server Configurations: Enumerate every BIG-IP APM virtual server that has both an access policy and an OAuth profile attached and determine whether APM is acting as an OAuth Authorization Server on it. These virtual servers, particularly those reachable from the internet, define the true exposure and should be prioritised for patching and threat hunting.



Deploy the Vendor Mitigation iRule Where Patching Is Delayed: If the hotfix cannot be installed immediately, contact F5 Support to obtain the iRule-based mitigation and apply it to every affected APM virtual server. Treat this strictly as a temporary control, validate that OAuth flows continue to function after it is applied, and retire it only once the hotfix is in place.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Execution	<u>T1059</u> : Command and Scripting Interpreter	



Patch Link

<https://my.f5.com/manage/s/article/K000162605>



References

<https://my.f5.com/manage/s/article/K000162605>

<https://cert.europa.eu/publications/security-advisories/2026-013/>



What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

September 23, 2026 • 08:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com