



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday September 24, 2026

CAL-CSIC-202609-A-011

Critical Buffer Overflow Vulnerability Affecting F5 BIG-IP Access Policy Manager

Remote Code Execution

No Authentication Required

Under Active Exploitation

F5 BIG-IP

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability affecting F5 BIG-IP Access Policy Manager (APM) instances configured as OAuth Authorization Servers. CVE-2026-94127 is a heap-based buffer overflow vulnerability (CWE-122) in the data plane OAuth handling logic that allows an unauthenticated remote attacker to execute arbitrary code with elevated privileges on the underlying operating system.¹ Exploitation requires no authentication, administrative credentials, or user interaction. The vulnerability carries a CVSS v3.1 base score of 9.8 (Critical)², and has been added to the CISA Known Exploited Vulnerabilities (KEV)³ catalog due to confirmed active exploitation in the wild. No verified public Proof-of-Concept (PoC) has been released.

The Cal-CSIC recommends the following:

1. Verify Updates: BIG-IP APM deployments as OAuth Authorization Servers and apply the hotfix corresponding to your release train (17.1.x, 17.5.x, or 21.x).
2. Apply Interim Mitigations: If hotfixing cannot be executed immediately, contact F5 Support to obtain and deploy the vendor-validated mitigation iRule across all exposed virtual servers.
3. Check for Indicators of Compromise: Inspect /var/log/apm for anomalous clusters of invalid_token authentication failures, evaluate tmctl global_oauth_stat failure metrics, and review any recent Traffic Management Microkernel (TMM) core dumps or unexpected outbound network connections originating from the data plane.

For more information, please see [F5 Advisory](#) for further details.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Components and Versions

Affected Product	Affected Branch	Versions Impacted
BIG-IP APM	21.x	21.1.0
	17.x	17.5.0-17.5.1 17.1.0-17.1.3

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References:

¹ F5; Security Advisory K000162605: BIG-IP APM vulnerability CVE-2026-94127; <https://my.f5.com/manage/s/article/K000162605>; Access 24 September 2026

² National Vulnerability Database (NVD); CVE-2026-94127 Details; <https://nvd.nist.gov/vuln/detail/cve-2026-94127>; Access 24 September 2026

³ CISA; Known Exploited Vulnerabilities Catalog; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-94127; Access 24 September 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR