An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609020277

NCSC Advisory

Critical Vulnerability in F5: BIG-IP APM

CVE-2026-94127

23rd, September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-94127

Published: 2026-09-22

Vendor: F5

Product: BIG-IP

CVSS Score[1]: 9.8

Products Affected

Product	Version
BIG-IP	21.1.0
BIG-IP	17.5.0 -17.5.1
BIG-IP	17.1.0 -17.1.3

Impact

When a BIG-IP APM access policy and an OAuth profile are configured on a virtual server, specific malicious traffic can lead to remote code execution (RCE). This vulnerability is only present when BIG-IP APM is configured as an OAuth Authorization Server. Deployments using APM strictly as an OAuth Client / Resource Server (without OAuth authorization server profiles configured) are not affected by this vulnerability.

This vulnerability allows an unauthenticated attacker to perform remote code execution. The BIG-IP system in Appliance mode is also vulnerable. This is a data plane issue; there is no control plane exposure.

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

Common Weakness Enumeration (CWE)[2]: CWE-122 Heap-based Buffer Overflow

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from F5.

- https://nvd.nist.gov/vuln/detail/CVE-2026-94127
- https://www.cve.org/CVERecord?id=CVE-2026-94127
- https://my.f5.com/manage/s/article/K000162605
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-94127

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog