

CVE-2025-53521

F5 BIG-IP Stack-Based Buffer Overflow Vulnerability

CISA KEV since Mar 27, 2026

Actively exploited

When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

EVRS 75/₁₀₀ Urgent priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.023 83.1st percentile · FIRST	CISA DEADLINE Mar 30, 2026 CISA federal deadline · Overdue by 7 months
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.023 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Please adhere to F5's guidelines to assess exposure and mitigate risks. Check for signs of potential compromise on all internet accessible F5 products affected by this vulnerability.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip access policy manager	≥ 15.1.0 < 15.1.10.8 ≥ 16.1.0 < 16.1.6.1 ≥ 17.1.0 < 17.1.3 ≥ 17.5.0 < 17.5.1.3	15.1.10.8 · 16.1.6.1 · 17.1.3 · 17.5.1.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-j3cp-7wh4-9f6c
my.f5.com my.f5.com/manage/s/article/K000160486
NVD nvd.nist.gov/vuln/detail/CVE-2025-53521

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-34630

Additional guidance my.f5.com/manage/s/article/K000156741
my.f5.com my.f5.com/manage/s/article/K11438344
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-53521

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.