BigIP APM Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-53521
State	PUBLISHED
Assigner	f5
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-15 14:15:48 UTC
Updated	2026-03-31 17:12:31 UTC
Description	When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Exe

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from f5sirt@f5.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.414080000 probability, percentile 0.973770000 (date 2026-04-01)

CISA KEV: Listed on 2026-03-27; due 2026-03-30; ransomware use Unknown

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	f5sirt@f5.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	f5sirt@f5.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	F5
Product	BIG-IP
Name	F5 BIG-IP Unspecified Vulnerability
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.
Notes	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. For more information please see: https://my.f5.com/manage/s/article/K000156741 ; https://my.f5.com/manage/s/article/K000160486 ; https://my.f5.com/manage/s/article/K11438344 ; https://nvd.nist.gov/vuln/detail/CVE-2025-53521

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	F5	BIG-IP	affected 17.5.0 17.5.1.3 custom	Not specified
CNA	F5	BIG-IP	affected 17.1.0 17.1.3 custom	Not specified
CNA	F5	BIG-IP	affected 16.1.0 16.1.6.1 custom	Not specified
CNA	F5	BIG-IP	affected 15.1.0 15.1.10.8 custom	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov	US Government Resourc
my.f5.com/manage/s/article/K000156741	f5sirt@f5.com	my.f5.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

Vendor Comments And Credit

Discovery Credit

CNA: F5 would like to thank Kristian Vlaardingerbroek, Hugo Trippaers, and other people of Schuberg Philis; Bart Vrancken; Fox-IT; and the National Cyber Security Centre (NCSC) in the Netherlands for their assistance in investigating this issue and following the highest standards of coordinated disclosure. (en)

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report