K000156572: Quarterly Security Notification (October 2025)

https://my.f5.com/manage/s/article/K000156572

Published Date: **Oct 15, 2025 UTC** Updated Date: **Oct 15, 2025 UTC**

Evaluated products

BIG-IP AAM : [15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP AFM : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP APM : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP ASM : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP Analytics : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP DDoS Hybrid Defender : [17.1.0, 16.1.0, 15.1.1, 15.1.0]

BIG-IP DNS : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP FPS : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP LTM : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP Link Controller : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP Next CGNAT CNF : [2.1.0, 2.0.2, 2.0.1, 2.0.0, 1.4.1, 1.4.0, 1.3.3, 1.3.2, 1.3.1, 1.3.0, 1.2.1, 1.2.0, 1.1.1, 1.1.0]

BIG-IP Next DNS CNF : [2.1.0, 2.0.2, 2.0.1, 2.0.0, 1.4.1, 1.4.0, 1.3.3, 1.3.2, 1.3.1, 1.3.0, 1.2.1, 1.2.0, 1.1.1, 1.1.0]

BIG-IP Next Edge Firewall CNF : [2.1.0, 2.0.2, 2.0.1, 2.0.0, 1.4.1, 1.4.0, 1.3.3, 1.3.2, 1.3.1, 1.3.0, 1.2.1, 1.2.0, 1.1.1, 1.1.0]

BIG-IP Next SPK : [2.0.2, 2.0.1, 2.0.0, 1.9.2, 1.9.1, 1.9.0, 1.8.2, 1.8.0, 1.7.14, 1.7.13, 1.7.12, 1.7.11, 1.7.10, 1.7.9, 1.7.8, 1.7.7, 1.7.6, 1.7.5, 1.7.4, 1.7.3, 1.7.2, 1.7.1, 1.7.0]

BIG-IP Next for Kubernetes : [2.1.0, 2.0.0]

BIG-IP PEM : [17.5.1, 17.5.0, 17.1.3, 17.1.2, 17.1.1, 17.1.0, 16.1.6, 16.1.5, 16.1.4, 16.1.3, 16.1.2, 16.1.1, 16.1.0, 15.1.10, 15.1.9, 15.1.8, 15.1.7, 15.1.6, 15.1.5, 15.1.4, 15.1.3, 15.1.2, 15.1.1, 15.1.0]

BIG-IP SSL Orchestrator : [17.5.0, 17.1.1, 17.1.0, 16.1.4, 16.1.3, 16.1.1, 16.1.0, 15.1.9, 15.1.2, 15.1.1, 15.1.0]

BIG-IQ Centralized Management : [8.4.0, 8.3.0]

F5 AI Gateway : [1.2.0, 1.1.1, 1.1.0, 1.0.2, 1.0.1, 1.0.0]

F5 Distributed Cloud Services

F5 Silverline

F5OS-A : [1.8.3, 1.8.0, 1.8.X, 1.5.4, 1.5.3, 1.5.2, 1.5.1, 1.5.0, 1.5.X]

F5OS-C : [1.8.2, 1.8.1, 1.8.0, 1.8.X, 1.6.4, 1.6.2, 1.6.1, 1.6.0, 1.6.X]

NGINX API Connectivity Manager : [1.9.3, 1.9.2, 1.9.1, 1.9.0, 1.8.0, 1.7.0, 1.6.0, 1.5.0, 1.4.1, 1.4.0, 1.3.1, 1.3.0]

NGINX Agent : [3.3.2, 3.3.1, 3.3.0, 3.2.1, 3.2.0, 3.1.0, 3.0.1, 3.0.0, 2.43.0, 2.42.2, 2.42.1, 2.42.0, 2.41.2, 2.41.1, 2.41.0, 2.40.1, 2.40.0, 2.39.0, 2.38.0, 2.37.0, 2.36.1, 2.36.0, 2.35.1, 2.35.0, 2.34.1, 2.34.0, 2.33.0, 2.32.2, 2.32.1, 2.32.0, 2.31.2, 2.31.1, 2.31.0, 2.30.3, 2.30.2, 2.30.1, 2.30.0]

NGINX App Protect DoS : [4.7.0, 4.6.0, 4.5.0, 4.4.0, 4.3.0, 4.2.0]

NGINX App Protect WAF : [5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.0, 5.3.0, 5.2.0, 5.1.0, 5.0.0, 4.16.0, 4.15.0, 4.14.0, 4.13.0, 4.12.0, 4.11.0, 4.10.0, 4.9.0, 4.8.1, 4.8.0, 4.7.0, 4.6.0, 4.5.0]

NGINX Controller : [3.22.9, 3.22.8, 3.22.7, 3.22.6, 3.22.5, 3.22.4, 3.22.3, 3.22.2, 3.22.1, 3.22.0, 3.21.0, 3.20.1, 3.20.0, 3.19.6-APIM, 3.19.5-APIM, 3.19.4-APIM, 3.19.3-APIM, 3.19.2-APIM, 3.19.1-APIM, 3.18.3]

NGINX Gateway Fabric : [2.1.2, 2.1.1, 2.1.0, 2.0.1, 2.0.0, 1.6.2, 1.6.1, 1.6.0, 1.5.1, 1.5.0, 1.4.0, 1.3.0, 1.2.0, 1.1.0, 1.0.0]

NGINX Ingress Controller : [5.2.1, 5.2.0, 5.1.1, 5.1.0, 5.0.0, 4.0.0, 3.7.1, 3.7.0, 3.6.2, 3.6.1, 3.6.0, 3.5.2, 3.5.1, 3.5.0, 3.4.2, 3.4.1, 3.4.0, 3.3.1]

NGINX Instance Manager : [2.20.0, 2.19.2, 2.19.1, 2.19.0, 2.18.0, 2.17.4, 2.17.3, 2.17.2, 2.17.1, 2.17.0, 2.16.0, 2.15.1, 2.15.0, 2.14.1, 2.14.0, 2.13.1, 2.13.0, 2.12.0]

NGINX Management Suite Security Monitoring : [1.7.1, 1.7.0, 1.6.0, 1.5.0, 1.4.0, 1.3.0, 1.2.0, 1.1.0, 1.0.0]

NGINX One Console

NGINX Open Source

NGINX Plus : [R35, R34, R33, R32, R31]

NGINX Service Mesh : [2.0.0, 1.7.0, 1.6.0, 1.5.0, 1.4.1, 1.4.0, 1.3.1, 1.3.0, 1.2.1, 1.2.0, 1.1.0]

NGINX Unit : [1.35.0, 1.34.2, 1.34.1, 1.34.0, 1.33.0, 1.32.1, 1.32.0, 1.31.1]

Traffix SDC : [5.2.0]

Security Advisory Description

On October 15, 2025, F5 announced the following security issues. This document is intended to serve as an overview of these vulnerabilities and security exposures to help determine the impact to your F5 devices. You can find the details of each issue in the associated articles.

- **High CVEs**
- **Medium CVEs**
- **Low CVEs**
- **Security Exposures**

High CVEs

Article (CVE)	CVSS score[1]	Affected products	Affected versions[2]	Fixes introduced in
K000151902: BIG-IP SCP and SFTP vulnerability CVE-2025-53868	8.7 (CVSS v3.1) 8.5 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.3 16.1.6.1 15.1.10.8
K000156767: F5OS vulnerability CVE-2025-61955	7.8 (standard mode) (CVSS v3.1) 8.8 (appliance mode) (CVSS v3.1) 8.5 (standard and appliance mode) (CVSS v4.0)	F5OS-A	1.8.0[3] 1.5.1 - 1.5.3	1.8.3 1.5.4
		F5OS-C	1.8.0 - 1.8.1 1.6.0 - 1.6.2[3]	1.8.2 1.6.4
K000156771: F5OS vulnerability CVE-2025-57780	7.8 (standard mode) (CVSS v3.1) 8.8 (appliance mode) (CVSS v3.1) 8.5 (standard and appliance mode) (CVSS v4.0)	F5OS-A	1.8.0[3] 1.5.1 - 1.5.3	1.8.3 1.5.4
		F5OS-C	1.8.0 - 1.8.1 1.6.0 - 1.6.2[3]	1.8.2 1.6.4
K000139514: BIG-IP SSL/TLS vulnerability CVE-2025-60016	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
		BIG-IP Next SPK	1.7.0 - 1.9.2	2.0.0
		BIG-IP Next CNF	1.1.0 - 1.3.3	2.0.0 1.4.0
		BIG-IP (all	17.1.0 - 17.1.2 16.1.0 -	17.1.2.2

K000150614: BIG-IP MPTCP vulnerability CVE-2025-48008	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	modules)	16.1.5 15.1.0 - 15.1.10	16.1.6 15.1.10.8
		BIG-IP Next SPK	1.7.0 - 1.9.2	None
		BIG-IP Next CNF	1.1.0 - 1.4.1	None
K000150637: BIG-IP DNS cache vulnerability CVE-2025-59781	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.1.0 - 17.1.2 16.1.0 - 16.1.5 15.1.0 - 15.1.10	17.1.2.2 16.1.6 15.1.10.8
		BIG-IP Next CNF	1.1.0 - 1.4.0	1.4.0 EHF-3[4]
K000150667: BIG-IP SSL Orchestrator vulnerability CVE-2025-41430	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP SSL Orchestrator	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.3 15.1.0 - 15.1.9	17.5.1 17.1.3 16.1.4
K000150752: BIG-IP HTTP/2 vulnerability CVE-2025-55669	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP ASM	17.1.0 - 17.1.2 16.1.0 - 16.1.5	17.1.2.2 16.1.6
K000151309: BIG-IP DTLS 1.2 vulnerability CVE-2025-61951	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6	17.5.1 17.1.3 16.1.6.1
K000151368: BIG-IP SSL Orchestrator vulnerability CVE-2025-55036	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP SSL Orchestrator	17.1.0 - 17.1.2 16.1.0 - 16.1.5 15.1.0 - 15.1.10	17.1.3 16.1.6 15.1.10.8
		BIG-IP PEM	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.3 16.1.6.1 15.1.10.8
				2.1.0

K000151475: BIG-IP PEM vulnerability CVE-2025-54479	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Next CNF	2.0.0 - 2.1.0 1.1.0 - 1.4.0	EHF-1[4] 2.0.2 EHF-2[4] 2.0.0 EHF-2[4] 1.4.0 EHF-3[4]
		BIG-IP Next for Kubernetes	2.0.0 - 2.1.0	2.1.0 EHF-2[4]
K000151611: BIG-IP iRules vulnerability CVE-2025-46706	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.1.0 - 17.1.2 16.1.0 - 16.1.5	17.1.2.2 16.1.6
		BIG-IP Next SPK	1.7.0 - 1.9.2	2.0.0 1.7.14 EHF-2[4]
		BIG-IP Next CNF	1.1.0 - 1.4.1	2.0.0 1.4.0 EHF-3[4]
K000152341: BIG-IP AFM DoS protection profile vulnerability CVE-2025-59478	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP AFM	17.5.0 17.1.0 - 17.1.2 15.1.0 - 15.1.10	17.5.1 17.1.3 15.1.10.8
K000156624: BIG-IP Advanced WAF and ASM bd process vulnerability CVE-2025-61938	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Advanced WAF/ASM	17.5.0 17.1.0 - 17.1.2	17.5.1 17.1.3
K000156621: BIG-IP Advanced WAF and ASM vulnerability CVE-2025-54858	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Advanced WAF/ASM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000156623: BIG-IP Next (CNF, SPK, and Kubernetes) vulnerability CVE-2025-58120	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Next SPK	2.0.0 1.7.0 - 1.7.14	2.0.1 1.7.14 EHF-2[4]
		BIG-IP Next CNF	2.0.0 1.1.0 - 1.4.1	2.0.1
		BIG-IP Next for Kubernetes	2.0.0	2.1.0

K000156707: BIG-IP TMM vulnerability CVE-2025-53856	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000156733: BIG-IP SSL/TLS vulnerability CVE-2025-61974	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
		BIG-IP Next SPK	2.0.0 - 2.0.2 1.7.0 - 1.9.2	2.1.0 EHF-1[4] 2.0.2 EHF-2[4] 2.0.0 EHF-2[4] 1.7.14 EHF-2[4]
		BIG-IP Next CNF	2.0.0 - 2.1.0 1.1.0 - 1.4.1	2.1.0 EHF-1[4] 2.0.2 EHF-2[4] 2.0.0 EHF-2[4] 1.4.0 EHF-3[4]
		BIG-IP Next for Kubernetes	2.0.0 - 2.1.0	2.1.0 EHF-1[4]
	3.7 (CVSS v3.1) 6.3 (CVSS v4.0)	F5 Silverline (all services)	Not applicable	Not applicable
K000156746: BIG-IP IPsec vulnerability CVE-2025-58071	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.3 16.1.6.1 15.1.10.8
			2.0.0 -	2.1.0 EHF-1[4] 2.0.2

		BIG-IP Next CNF	2.1.0 1.1.0 - 1.4.1	EHF-2[4] 2.0.0 EHF-2[4] 1.4.0 EHF-3[4]
		BIG-IP Next for Kubernetes	2.0.0 - 2.1.0	2.1.0 EHF-1[4]
K000156741: BIG-IP APM vulnerability CVE-2025-53521	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP APM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000156597: BIG-IP APM portal access vulnerability CVE-2025-61960	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP APM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6	17.5.1.3 17.1.3 16.1.6.1
K000156602: BIG-IP APM vulnerability CVE-2025-54854	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP APM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K44517780: BIG-IP iRules vulnerability CVE-2025-53474	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP APM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
		BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
				2.1.0

K000156912: BIG-IP TMM vulnerability CVE-2025-61990	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Next SPK	2.0.0 - 2.0.2 1.7.0 - 1.9.2	EHF-1[4] 2.0.2 EHF-2[4] 2.0.0 EHF-2[4] 1.7.15 EHF-2[4]
		BIG-IP Next CNF	2.0.0 - 2.1.0 1.1.0 - 1.4.1	2.1.0 EHF-1[4] 2.0.2 EHF-2[4] 2.0.0 EHF-2[4] 1.4.0 EHF-3[4]
		BIG-IP Next for Kubernetes	2.0.0 - 2.1.0	2.1.0 EHF-1[4]
K000156691: BIG-IP TMM vulnerability CVE-2025-58096	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000154664: BIG-IP Advanced WAF and ASM vulnerability CVE-2025-61935	7.5 (CVSS v3.1) 8.7 (CVSS v4.0)	BIG-IP Advanced WAF/ASM	17.5.0 17.1.0 - 17.1.2 15.1.0 - 15.1.10	17.5.1 17.1.3 15.1.10.8
K000151718: VELOS partition container network vulnerability CVE-2025-59778	7.5 (CVSS v3.1) 7.7 (CVSS v4.0)	F5OS-C	1.8.0 - 1.8.1 1.6.0 - 1.6.2[3]	1.8.2 1.6.4

[1]Starting with the August 2024 Quarterly Security Notification, F5 will provide the CVSS v4.0 base score in addition to the CVSS v3.1 score, for first-party security issues only. For more information about how F5 uses CVSS v4.0, refer to ***K000140363: Overview of CVSS v4.0 in F5 security advisories****.*

[2]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.

[3]F5OS-A 1.8.1, F5OS-A 1.8.2, and F5OS-C 1.6.3 are excluded from MyF5 Downloads. For more information, refer to ***K46066337: Certain F5 software releases are not publicly available****.*

[4]F5 has fixed this issue in an engineering hotfix that is available from the ***MyF5 Downloads*** *page. For more information, refer to* ***K000090258: Download F5 products from MyF5****. While F5 endeavors to release the most stable code possible, engineering hotfixes do not undergo the extensive QA assessment of scheduled software releases. F5 offers*

*engineering hotfixes with no warranty or guarantee of usability. For more information about the hotfix policy, refer to **K4918: Overview of the F5 critical issue hotfix policy**.*

Medium CVEs

Article (CVE)	CVSS score[1]	Affected products	Affected versions [2]	Fixes introduced in
K000156642: BIG-IP iControl REST and tmsh vulnerability CVE-2025-59481	6.5 (standard mode) (CVSS v3.1) 8.7 (appliance mode) (CVSS v3.1) 8.5 (standard and appliance mode) (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000154647: BIG-IP tmsh vulnerability CVE-2025-61958	6.5 (standard mode) (CVSS v3.1) 8.7 (appliance mode) (CVSS v3.1) 8.5 (standard and appliance mode) (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.1 17.1.3 16.1.6.1 15.1.10.8
K000148816: BIG-IP APM and SSL Orchestrator vulnerability CVE-2025-47148	6.5 (CVSS v3.1) 7.1 (CVSS v4.0)	BIG-IP APM, APM with SWG, SSL Orchestrator, SSL Orchestrator with SWG	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.3 16.1.6.1 15.1.10.8
K000149820: F5OS SNMP vulnerability CVE-2025-47150	6.5 (CVSS v3.1) 7.1 (CVSS v4.0)	F5OS-A	1.8.0 - 1.8.1[3] 1.5.1 - 1.5.2	1.8.3 1.5.3
		F5OS-C	1.6.0 - 1.6.2[3]	1.8.0 1.6.4
K000154614: BIG-IP Next (CNF, SPK, and Kubernetes) vulnerability CVE-2025-55670	6.5 (CVSS v3.1) 7.1 (CVSS v4.0)	BIG-IP Next SPK	1.7.0 - 1.9.2	None
		BIG-IP Next CNF	1.1.0 - 1.4.1	None
		BIG-IP Next for Kubernetes	2.0.0	2.1.0

K000151596: BIG-IP TMM vulnerability CVE-2025-54805	6.5 (CVSS v3.1) 6.0 (CVSS v4.0)	BIG-IP Next SPK	1.7.0 - 1.9.2	2.0.0
		BIG-IP Next CNF	1.1.0 - 1.4.1	2.0.0
		BIG-IP Next for Kubernetes	2.0.0	2.1.0
K000151308: BIG-IP Configuration utility XSS vulnerability CVE-2025-59269	6.1 (CVSS v3.1) 8.4 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.3 16.1.6.1 15.1.10.8
K000151658: BIG-IP HSB vulnerability CVE-2025-58153	5.9 (CVSS v3.1) 8.2 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1 17.1.0 16.1.6.1 15.1.10.8
K000156796: F5OS out-of-bounds write vulnerability CVE-2025-60015	5.7 (CVSS v3.1) 6.9 (CVSS v4.0)	F5OS-A	1.8.0[3] 1.5.1 - 1.5.3	1.8.3 1.5.4
		F5OS-C	1.8.0 - 1.8.1 1.6.0 - 1.6.2[3]	1.8.2 1.6.4
K000156800: BIG-IP Configuration utility vulnerability CVE-2025-59483	6.5 (CVSS v3.1) 8.5 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000154661: F5OS-A FIPS HSM password vulnerability CVE-2025-60013	5.7 (CVSS v3.1) 4.6 (CVSS v4.0)	F5OS-A	1.8.0[3] 1.5.1 - 1.5.3	1.8.3 1.5.4
K90301300: BIG-IP Configuration utility vulnerability CVE-2025-59268	5.3 (CVSS v3.1) 6.9 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000148512: BIG-IP Advanced WAF and	5.3 (CVSS v3.1)	BIG-IP Advanced WAF/ASM	17.1.0 - 17.1.1	17.1.2

ASM and NGINX App Protect DNS lookup vulnerability CVE-2025-58474	6.9 (CVSS v4.0)	NGINX App Protect WAF	4.5.0 - 4.6.0	4.7.0
K000156596: BIG-IP APM XSS vulnerability CVE-2025-61933	6.1 (CVSS v3.1) 5.1 (CVSS v4.0)	BIG-IP APM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000156801: BIG-IP Configuration utility vulnerability CVE-2025-54755	4.9 (CVSS v3.1) 6.9 (CVSS v4.0)	BIG-IP (all modules)	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.3 17.1.3 16.1.6.1 15.1.10.8
K000148625: F5OS-A FIPS HSM vulnerability CVE-2025-53860	4.1 (CVSS v3.1) 5.6 (CVSS v4.0)	F5OS-A	1.8.0[3] 1.5.1 - 1.5.2	1.8.3 1.5.3

*[1]Starting with the August 2024 Quarterly Security Notification, F5 will provide the CVSS v4.0 base score in addition to the CVSS v3.1 score, for first-party security issues only. For more information about how F5 uses CVSS v4.0, refer to **K000140363: Overview of CVSS v4.0 in F5 security advisories**.*

[2]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.

*[3]F5OS-A 1.8.1, F5OS-A 1.8.2, and F5OS-C 1.6.3 are excluded from MyF5 Downloads. For more information, refer to **K46066337: Certain F5 software releases are not publicly available**.*

Low CVEs

Article (CVE)	CVSS score [1]	Affected products	Affected versions[2]	Fixes introduced in
K000151297: BIG-IP TMM vulnerability CVE-2025-58424	3.7 (CVSS v3.1) 6.3 (CVSS v4.0)	BIG-IP (all modules)	17.1.0 - 17.1.2 16.1.0 - 16.1.5 15.1.0 - 15.1.10	17.1.2.2[3] 16.1.6[3] 15.1.10.8[3]
	3.1 (CVSS v3.1) 2.3 (CVSS v4.0)	F5 Silverline (all services)	Not applicable	Not applicable

*[1]Starting with the August 2024 Quarterly Security Notification, F5 will provide the CVSS v4.0 base score in addition to the CVSS v3.1 score, for first-party security issues only. For more information about how F5 uses CVSS v4.0, refer to **K000140363: Overview of CVSS v4.0 in F5 security advisories**.*

[2]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.

*[3]To mitigate this issue, in addition to installing a fixed version, you must also enable the **tm.tcpstopblindinjection** database variable.*

Security Exposures

Article (Exposure)	Affected products	Affected versions[1]	Fixes introduced in
K000150010: BIG-IP AFM security exposure	BIG-IP AFM	17.5.0 - 17.5.1 17.1.0 - 17.1.2 16.1.0 - 16.1.6 15.1.0 - 15.1.10	17.5.1.1 17.1.3

[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle.

Related Content

Frequently used QSN articles

- **K5903: BIG-IP software support policy**
- **K4309: F5 hardware product lifecycle support policy**
- **K9476: The F5 hardware/software compatibility matrix**
- **K13845: Overview of supported BIG-IP upgrade paths and an upgrade planning reference**
- **K000157005: F5 signing certificate and key rotation, October 2025**

Security best practices

- **K53108777: Hardening your F5 system**
- **K45321906: Harden your BIG-IQ system**
- **K000156803: Hardening NGINX and NGINX Plus**
- **Secure the AOM subsystem**
- **DevCentral: Security Best Practices for F5 Products**

Other helpful resources

- **K12201527: Overview of Quarterly Security Notifications**
- **K67091411: Guidance for Quarterly Security Notifications**
- **K84205182: BIG-IP update and upgrade guide | Chapter 1: Guide contents**
- **K41942608: Overview of MyF5 security advisory articles**
- **K4602: Overview of the F5 security vulnerability response policy**
- **K4918: Overview of the F5 critical issue hotfix policy**
- **K39757430: F5 product and services lifecycle policy index**
- **K9502: BIG-IP hotfix and point release matrix**
- **K13123: Managing BIG-IP product hotfixes (11.x - 17.x)**
- **K48955220: Installing an OPSWAT Endpoint Security update on BIG-IP APM systems (11.4.x and later)**

- **K000090258: Download F5 products from MyF5**
- **K9970: Subscribe to email notifications regarding F5 products and security announcements**
- **K9957: Creating a custom RSS feed to view new and updated documents**
- **K27404821: Using F5 iHealth to diagnose vulnerabilities**
- **K000135931: Contact F5 Support**