

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates- F5 Products
Tracking #:432317234
Date:09-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed F5 Networks has released multiple security updates to address a series of vulnerabilities affecting its BIG-IP and BIG-IP Next Central Manager products.

TECHNICAL DETAILS:

F5 Networks has released multiple security updates to address a series of vulnerabilities affecting its BIG-IP and BIG-IP Next Central Manager products.

Vulnerability Details:

(CVE)	CVSS score	Affected products	Affected versions	Fixes introduced in
K000139503: F5OS vulnerability CVE-2025-46265	8.8 (CVSS v3.1)	F5OS-A	1.5.1	1.8.0
	8.7 (CVSS v4.0)			1.5.2
		F5OS-C	1.6.0 - 1.6.2	1.8.0
K000148591: Appliance mode BIG-IP iControl REST and tmsh vulnerability CVE-2025-31644	8.7 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.2	17.1.2.2
	8.5 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.6
			15.1.0 - 15.1.10	15.1.10.7
K000140574: F5OS Appliance Mode vulnerability CVE-2025-36546	8.1 (CVSS v3.1)	F5OS-A	1.5.1 - 1.5.2	1.8.0
	9.2 (CVSS v4.0)			1.5.3
		F5OS-C	1.6.0 - 1.6.2	1.8.0
K000137709: SCTP vulnerability CVE-2025-41399	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0	17.1.1
	8.7 (CVSS v4.0)		16.1.0 - 16.1.3	16.1.4
			15.1.0 - 15.1.8	15.1.9
		BIG-IP Next (all modules)	20.2.0	20.2.1
		BIG-IP Next SPK	1.8.0 - 1.9.2	2.0.0
			1.7.0 - 1.7.11	1.7.12
		BIG-IP Next CNF	1.1.0 - 1.2.1	1.3.0
K000139571: BIG-IP HTTP vulnerability CVE-2025-36557	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.4	16.1.5
		BIG-IP Next SPK	1.8.0 - 1.9.2	2.0.0
			1.7.0 - 1.7.8	1.7.9
		BIG-IP Next CNF	1.1.0 - 1.3.3	2.0.0
				1.4.0



K000140919: BIG-IP HTTP/2 vulnerability CVE-2025-36504	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.6
		BIG-IP Next (all modules)	20.2.0 - 20.2.1	20.3.0
		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
K000140937: BIG-IP SIP ALG profile vulnerability CVE-2025-41433	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.4	16.1.5
			15.1.0 - 15.1.10	
K000140968: BIG-IP HTTP/2 vulnerability CVE-2025-41414	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.4	16.1.5
			15.1.0 - 15.1.10	
		BIG-IP Next SPK	1.8.0 - 1.9.2	2.0.0
			1.7.0 - 1.7.8	1.7.9
		BIG-IP Next CNF	1.1.0 - 1.3.3	2.0.0
				1.4.0
K000150598: BIG-IP APM PingAccess vulnerability CVE-2025-36525	7.5 (CVSS v3.1)	BIG-IP (APM)	17.1.0 - 17.1.2	17.1.2.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.6
			15.1.0 - 15.1.10	
K000149952: BIG-IP PEM vulnerability CVE-2025-35995	7.5 (CVSS v3.1)	BIG-IP (PEM)	17.1.0 - 17.1.2	17.1.2.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.6
			15.1.0 - 15.1.10	
K000150668: TMM vulnerability CVE-2025-41431	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.2	17.1.2.2
	8.7 (CVSS v4.0)			

Medium Severity:

CVE	CVSS v3.1	Product	Affected Versions	Fixed In
CVE-2025-43878	6.0	F5OS-A / F5OS-C	A: 1.5.1-1.5.3 / C: 1.6.0-1.6.2	1.8.0

RECOMMENDATIONS:

- Update to the fixed versions. If patching is not immediately possible, apply any F5-provided mitigation guidance until updates can be deployed.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://my.f5.com/manage/s/article/K000151008?utm_source=f5support&utm_medium=RSS#medium