مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

F5 Networks Quarterly Security Updates

Tracking #:432316832

Date:06-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that F5 Networks released its Quarterly Security Notification, disclosing multiple vulnerabilities affecting various F5 products, including BIG-IP, BIG-IP Next, and NGINX.

TECHNICAL DETAILS:

On February 5, 2025, F5 Networks released its Quarterly Security Notification, disclosing multiple vulnerabilities affecting various F5 products, including BIG-IP, BIG-IP Next, and NGINX. The vulnerabilities range in severity from low to high, with several critical issues that could lead to remote code execution, privilege escalation, and denial of service.

High CVEs:

CVE	CVSS score	Affected products	Affected versions	Fixes introduced in
BIG-IP iControl REST and tmsh vulnerability CVE-2025-20029	8.8 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.2	17.1.2.1
	8.7 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.5.2
			15.1.0 - 15.1.10	15.1.10.6
BIG-IP iControl REST vulnerability CVE-2025-23239	8.7 (CVSS v3.1)	BIG-IP (all modules)	17.1.1	17.1.2
	8.5 (CVSS v4.0)			
BIG-IP Configuration utility vulnerability CVE-2025-24320	8.0 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	5.1 (CVSS v4.0)		16.1.0 - 16.1.5	16.1.5.2
			15.1.0 - 15.1.10	15.1.10.6
TMM vulnerability CVE-2025-21087	7.5 (CVSS v3.1)	BIG-IP (all modules)	17.1.0 - 17.1.1	17.1.2
	8.9 (CVSS v4.0)		16.1.0 - 16.1.5	Hotfix-BIGIP-16.1.5.2.0.7.5-ENG.iso
			15.1.0 - 15.1.10	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso

BIG-IP SIP ALG profile vulnerability CVE-2025-20045	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	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
BIG-IP SIP ALG vulnerability CVE-2025-22846	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	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
		BIG-IP Next SPK	1.9.0	1.9.1
			1.8.0 - 1.8.2	1.7.7
			1.7.0 - 1.7.6	
BIG-IP PEM vulnerability CVE-2025-22891	7.5 (CVSS v3.1)	BIG-IP (PEM)	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	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
BIG-IP PEM vulnerability CVE-2025-24497	7.5 (CVSS v3.1)	BIG-IP (PEM)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)			
BIG-IP SNMP vulnerability CVE-2025-21091	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	Hotfix-BIGIP-16.1.5.2.0.7.5-ENG.iso
			15.1.0 - 15.1.10	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
BIG-IP message routing vulnerability CVE-2025-20058	7.5 (CVSS v3.1)		17.1.0 - 17.1.1	17.1.2

	8.9 (CVSS v4.0)	BIG-IP (all modules)	16.1.0 - 16.1.5	Hotfix-BIGIP-16.1.5.2.0.7.5-ENG.iso
			15.1.0 - 15.1.10	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
BIG-IP ASM BADoS vulnerability CVE-2025-24326	7.5 (CVSS v3.1)	BIG-IP (ASM)	17.1.0 - 17.1.1	17.1.2
	8.9 (CVSS v4.0)		16.1.0 - 16.1.4	16.1.5
			15.1.0 - 15.1.10	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
BIG-IP APM access profile vulnerability CVE-2025-23412	7.5 (CVSS v3.1)	BIG-IP (APM)	16.1.3 - 16.1.4	16.1.5
	8.7 (CVSS v4.0)			
BIG-IP AFM vulnerability CVE-2025-24312	7.5 (CVSS v3.1)	BIG-IP (AFM)	17.1.0 - 17.1.1	17.1.2
	8.7 (CVSS v4.0)		16.1.0 - 16.1.5	Hotfix-BIGIP-16.1.5.2.0.7.5-ENG.iso
			15.1.0 - 15.1.10	Hotfix-BIGIP-15.1.10.6.0.11.6-ENG.iso
		BIG-IP Next CNF	1.1.0 - 1.3.3	1.4.0

Medium CVEs:

CVE	CVSS score	Affected products	Affected versions	Fixes introduced in
BIG-IP Next Central Manager vulnerability CVE-2025-24319	6.5 (CVSS v3.1) 7.1 (CVSS v4.0)	BIG-IP Next Central Manager	20.2.0 - 20.2.1	20.3.0
BIG-IP Next Central Manager logging vulnerability CVE-2025-23413	4.4 (CVSS v3.1) 6.7 (CVSS v4.0)	BIG-IP Next Central Manager	20.2.0 - 20.2.1	20.3.0
NGINX TLS session resumption vulnerability CVE-2025-23419	4.3 (CVSS v3.1) 5.3 (CVSS v4.0)	NGINX Plus	R28 - R33	R33 P2 R32 P2

		NGINX Open Source	1.11.4 - 1.27.3	1.27.4 1.26.3

RECOMMENDATIONS:

- Organizations using affected versions of BIG-IP, BIG-IP Next Central Manager, or NGINX should immediately upgrade to the fixed versions provided in the advisory to mitigate potential risks.

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/K000149540?utm_source=f5support&utm_medium=RSS