ADV2026_194 F5 Security Advisory (March 30th, 2026)

F5 published a security advisory highlighting vulnerabilities in multiple products on October 15th, 2025. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- BIG-IP (all modules) – versions 17.5.0 to 17.5.1, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.6, versions 15.1.0 to 15.1.10
- BIG-IP AFM – version 17.5.0, versions 17.1.0 to 17.1.2, versions 15.1.0 to 15.1.10
- BIG-IP APM – versions 17.5.0 to 17.5.1, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.6, versions 15.1.0 to 15.1.10
- BIG-IP APM, APM with SWG, SSL Orchestrator, SSL Orchestrator with SWG – version 17.5.0, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.6, versions 15.1.0 to 15.1.10
- BIG-IP ASM – versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.5
- BIG-IP Advanced WAF/ASM – versions 17.5.0 to 17.5.1, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.6, versions 15.1.0 to 15.1.10
- BIG-IP Next CNF – versions 2.0.0 to 2.1.0, versions 1.1.0 to 1.4.1
- BIG-IP Next SPK – versions 2.0.0 to 2.1.0, versions 1.7.0 to 1.9.2
- BIG-IP Next for Kubernetes – versions 2.0.0 to 2.1.0
- BIG-IP PEM – version 17.5.0, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.6, versions 15.1.0 to 15.1.10
- BIG-IP SSL Orchestrator – version 17.5.0, versions 17.1.0 to 17.1.2, versions 16.1.0 to 16.1.5, versions 15.1.0 to 15.1.10
- F5OS-A – versions 1.8.0 to 1.8.1, versions 1.5.1 to 1.5.3
- F5OS-C – version 1.8.0 to 1.8.1, versions 1.6.0 to 1.6.2
- NGINX App Protect WAF – versions 4.5.0 to 4.6.0

F5 also published security incident K000154696 advising that threat actors exfiltrated files from BIG-IP products and they are not aware of active exploitation of any undisclosed F5 vulnerabilities on October 15, 2025.

Update 1

F5 indicates that CVE-2025-53521 has been exploited.

Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-53521 to their Known Exploited Vulnerabilities (KEV) Database on March 27, 2026.

For more information on these updates, you can follow these URL:

- K000156741: BIG-IP APM vulnerability CVE-2025-53521
- K000160486: Indicators of Compromise for c05d5254
- CISA KEV: CVE-2025-53521
- K000154696: F5 Security Incident
- K53108777: Hardening your F5 system
- F5 Quarterly Security Notification (October 2025)

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- K000156741: BIG-IP APM vulnerability CVE-2025-53521. (March 28, 2026). Retrieved from F5. https://my.f5.com/manage/s/article/K000156741
- K000160486: Indicators of Compromise for c05d5254. (March 27, 2026). Retrieved from F5 Edge. https://my.f5.com/manage/s/article/K000160486
- CISA KEV: CVE-2025-53521. (n.b.). Retrieved from F5 Edge. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-53521
- K000154696: F5 Security Incident. (October 22, 2026). Retrieved from MyF5. https://msrc.F5.com/update-guide/vulnerability/CVE-2026-21509
- K53108777: Hardening your F5 system. (November 13, 2026). Retrieved from MyF5. https://my.f5.com/manage/s/article/K53108777
- F5 Quarterly Security Notification (October 2025). (March 27, 2026). Retrieved from MyF5. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2026-21509
- F5 security advisory - Update 1. (March 27, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/f5-security-advisory-av25-669