Security Advisory

K000156741: BIG-IP APM vulnerability CVE-2025-53521

Published Date: **Oct 15, 2025** Updated Date: **Apr 1, 2026**

AI Recommended Content

Evaluated products:

Security Advisory Description

When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE). (CVE-2025-53521)

Important: We have learned that this vulnerability has been exploited. If your BIG-IP APM system is running a vulnerable version, or was upgraded from one, please do the following actions:
- Review K000160486: Indicators of Compromise for c05d5254.
- If compromise is suspected, review K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system.

Impact

This is an issue impacting BIG-IP APM systems.

This vulnerability allows an unauthenticated attacker to perform remote code execution. The BIG-IP system in Appliance mode is also vulnerable. This is a data plane issue; there is no control plane exposure.

Note: This known vulnerability was previously categorized and remediated as a Denial-of-Service (DoS) vulnerability with CVSS scores of 7.5 (CVSS v3.1) and 8.7 (CVSS v4.0).

> Due to new information obtained in March 2026, the original vulnerability is being re-categorized to an RCE with CVSS scores of 9.8 (CVSS v3.1) and 9.3 (CVSS v4.0).
>
> The original CVE remediation has been validated to address the RCE in the fixed versions listed below.

Security Advisory Status

F5 Product Development has assigned ID 1977933 (BIG-IP APM) to this vulnerability. This issue has been classified as CWE-121: Stack-based Buffer Overflow.

To determine if your product and version have been evaluated for this vulnerability, refer to the **evaluated products** box. To determine if your release is known to be vulnerable, the components or features that are affected by the vulnerability, and for information about releases, point releases, or hotfixes that address the vulnerability, refer to the tables below. You can also use **iHealth** to diagnose a vulnerability for BIG-IP, BIG-IQ, and F5OS systems. For more information about using iHealth, refer to **K27404821: Using F5 iHealth to diagnose vulnerabilities**. For more information about security advisory versioning, refer to **K51812227: Understanding security advisory versioning**.

In this section

BIG-IP Next

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
BIG-IP Next SPK	All	None	Not applicable	Not vulnerable	None
BIG-IP Next CNF	All	None	Not applicable	Not vulnerable	None
BIG-IP Next for Kubernetes	All	None	Not applicable	Not vulnerable	None

*[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle. For more information, refer to the **Security hotfixes** section of **K4602: Overview of the F5 security vulnerability response policy**.*

BIG-IP and BIG-IQ

***Note**: After F5 releases a fix for a given branch, that fix applies to all subsequent minor, maintenance, and point releases for that branch; F5 will not list additional fixes for that branch in the table. For example, when F5 releases a fix in 17.1.2.1, the fix also applies to 17.1.2.2 and all later 17.1.x releases (17.1.3.x, 17.1.4.x). For more information, refer to **K51812227: Understanding security advisory versioning**.*

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity/CVSS score[2]	Vulnerable component or feature

BIG-IP APM	17.x	17.5.0 - 17.5.1 17.1.0 - 17.1.2	17.5.1.3 17.1.3	**Critical/9.8**[3] (CVSS v3.1) **Critical/9.3**[3] (CVSS v4.0)	The **apmd** process
	16.x	16.1.0 - 16.1.6	16.1.6.1		
	15.x	15.1.0 - 15.1.10	15.1.10.8		
BIG-IP (all other modules)	All	None	Not applicable	Not vulnerable	None
BIG-IQ Centralized Management	All	None	Not applicable	Not vulnerable	None

*[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle. For more information, refer to the **Security hotfixes** section of **K4602: Overview of the F5 security vulnerability response policy**.*

*[2]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. The CVSS score link takes you to a resource outside of MyF5, and the content may be removed without our knowledge. For more information about how F5 uses CVSS v4.0, refer to **K000140363: Overview of CVSS v4.0 in F5 security advisories**.*

[3]This known vulnerability was previously categorized and remediated as a DoS vulnerability with CVSS scores of 7.5 (CVSS v3.1) and 8.7 (CVSS v4.0). Due to new information obtained in March 2026, the original vulnerability is being re-categorized to an RCE with CVSS scores of 9.8 (CVSS v3.1) and 9.3 (CVSS v4.0). The original CVE remediation has been validated to address the issue for the recategorized RCE for the fixed versions listed above.

F5 Distributed Cloud and NGINX Services

Service	Severity/CVSS score	Vulnerable component or feature
F5 Distributed Cloud (all services)	Not vulnerable	None
F5 Silverline (all services)	Not vulnerable	None
NGINX One Console	Not vulnerable	None

F5OS

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
F5OS-A	All	None	Not applicable	Not vulnerable	None
F5OS-C	All	None	Not applicable	Not vulnerable	None

*[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle. For more information, refer to the **Security hotfixes** section of **K4602: Overview of the F5 security vulnerability response policy**.*

NGINX

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
NGINX (all products)	All	None	Not applicable	Not vulnerable	None

*[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle. For more information, refer to the **Security hotfixes** section of **K4602: Overview of the F5 security vulnerability response policy**.*

Other products

Product	Branch	Versions known to be vulnerable[1]	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
Traffix SDC	All	None	Not applicable	Not vulnerable	None
F5 AI Gateway	All	None	Not applicable	Not vulnerable	None

*[1]F5 evaluates only software versions that have not yet reached the End of Technical Support (EoTS) phase of their lifecycle. For more information, refer to the **Security hotfixes** section of **K4602: Overview of the F5 security vulnerability response policy**.*

Security Advisory Recommended Actions

If you are running a version listed in the **Versions known to be vulnerable** column, you can eliminate this vulnerability by installing a version listed in the **Fixes introduced in** column. If the **Fixes introduced in** column does not list a version for your branch, then no update candidate currently exists for that branch and F5 recommends that you upgrade to a version with the fix (refer to the tables).

If the **Fixes introduced in** column lists a version prior to the one you are running, in the same branch, then your version should have the fix.

Important: We have learned that this vulnerability has been exploited. If your BIG-IP APM system is running a vulnerable version, or was upgraded from one, please consider the following actions:
- Review **K000160486: Indicators of Compromise for c05d5254**.
- If compromise is suspected, review **K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system**.

Important: F5 strongly recommends that customers consult their corporate security policy for guidelines about incident handling procedures including but not limited to forensic best practices, that are specific to their organization. More specifically, that customers review their policies to ensure that they comply with evidence collection and forensics procedures for a security incident before attempting to recover the system. Additionally, if customers do not know exactly when the system was compromised, user configuration set (UCS) backups may have been created after the compromise occurred. F5 strongly recommends that customers rebuild the configuration from a known good source because UCS files from compromised systems can contain persistent malware.

Mitigation

None

Acknowledgments

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.

Related Content

- K41942608: Overview of MyF5 security advisory articles
- K12201527: Overview of Quarterly Security Notifications
- K51812227: Understanding security advisory versioning
- 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)
- 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
- K44525501: Overview of BIG-IP data plane and control plane
- K000135931: Contact F5 Support

AI Recommended Content

- Policy - K4309: F5 hardware product lifecycle support policy
- Security Advisory - K12201527: Overview of Quarterly Security Notifications
- Knowledge - K000135931: Contact F5 Support
- Security Advisory - K000161061: crypto: algif_aead - Revert to operating out-of-place (Copy Fail) CVE-2026-31431

Return to Top

Deliver and Secure Every App

F5 application delivery and security solutions are built to ensure that every app and API deployed anywhere is fast, available, and secure. Learn how we can partner to deliver exceptional experiences every time.

WHAT WE OFFER

RESOURCES

SUPPORT

PARTNERS

COMPANY

CONNECT WITH US

CONTACT SUPPORT