

[SIGN IN](#)

 Security Advisory



 [AI Recommended Content](#)

# K000150598: BIG-IP APM PingAccess vulnerability CVE-2025-36525

Published Date: May 7, 2025      Updated Date: May 7, 2025

✓ Evaluated products:

## Security Advisory Description

When a BIG-IP APM PingAccess profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. ([CVE-2025-36525](#))

## Impact

Traffic is disrupted while the TMM process restarts. This vulnerability allows a remote attacker to cause a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only.

## Security Advisory Status

F5 Product Development has assigned ID 1708261 (BIG-IP) to this vulnerability. This issue has been classified as [CWE-120: Buffer Copy without Checking Size of Input \('Classic Buffer Overflow'\)](#).

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 following tables. 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](#)
- [BIG-IP and BIG-IQ](#)
- [F5 Distributed Cloud and NGINX Services](#)
- [F5OS](#)
- [NGINX](#)
- [Other products](#)

**BIG-IP Next**

**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 20.0.2, the fix also applies to 20.0.3 and all later 20.1.x releases. For more information, refer to [K51812227: Understanding security advisory versioning](#).

Product	Branch	Versions known to be vulnerable <sup>1</sup>	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
BIG-IP Next (all modules)	All	None	Not applicable	Not vulnerable	None
BIG-IP Next Central Manager	All	None	Not applicable	Not vulnerable	None
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

<sup>1</sup>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 <sup>1</sup>	Fixes introduced in	Severity/CVSS score <sup>2</sup>	Vulnerable component or feature
BIG-IP (APM)	17.x	17.1.0 - 17.1.2	17.1.2.2	<b>High/7.5</b> (CVSS v3.1) <b>High/8.7</b> (CVSS v4.0)	PingAccess virtual server
	16.x	16.1.0 - 16.1.5	16.1.6		
	15.x	15.1.0 - 15.1.10	None		
BIG-IP (all other modules)	17.x	None	Not applicable	Not vulnerable <sup>3</sup>	None
	16.x	None	Not applicable		
	15.x	None	Not applicable		
BIG-IQ Centralized Management	All	None	Not applicable	Not vulnerable	None

*<sup>1</sup>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](#).*

*<sup>2</sup>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](#).*

*<sup>3</sup>The specified products contain the affected code. However, F5 identifies the vulnerability status as Not vulnerable because the attacker cannot exploit the code in default, standard, or recommended configurations.*

**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 <sup>1</sup>	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

*<sup>1</sup>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 <sup>1</sup>	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
NGINX (all products)	All	None	Not applicable	Not vulnerable	None

*<sup>1</sup>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 <sup>1</sup>	Fixes introduced in	Severity/CVSS score	Vulnerable component or feature
Traffix SDC	All	None	Not applicable	Not vulnerable	None

<sup>1</sup>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.

## Mitigation

F5 recommends you configure the BIG-IP systems with high availability (HA) to lessen the impact of the vulnerability.

- Configure systems with HA clustering. For more information, refer to [K02234544: Manually setting up device service clustering](#).
- Configure the HA table to take specific actions. For more information, refer to [K9231: Overview of BIG-IP daemon heartbeat failsafe](#).

## Acknowledgments

This issue was discovered internally by F5.

## Related Content

- [K000151187: Does BIG-IP 17.5.0 contain the same security fixes as 17.1.x?](#)
- [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 \(11.x - 17.x\)](#)
- [K48955220: Installing an OPSWAT Endpoint Security update on BIG-IP APM systems \(11.4.x and later\)](#)
- [K000090258: Download F5 products from MyF5](#)
- [K9970: Subscribing to email notifications regarding F5 products](#)
- [K9957: Creating a custom RSS feed to view new and updated documents](#)
- [K44525501: Overview of BIG-IP data plane and control plane](#)

## AI Recommended Content

- Security Advisory - [K000151008: Quarterly Security Notification \(May 2025\)](#)
- Policy - [K4309: F5 hardware product lifecycle support policy](#)
- Security Advisory - [K000139571: BIG-IP HTTP vulnerability CVE-2025-36557](#)
- Security Advisory - [K000148591: Appliance mode BIG-IP iControl REST and tmsh vulnerability CVE-2025-31644](#)

[↑ Return to Top](#)

## Secure and Deliver Extraordinary Digital Experiences

F5's portfolio of automation, security, performance, and insight capabilities empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users. [Learn more >](#)

---

WHAT WE OFFER

---

RESOURCES

---

SUPPORT

---

PARTNERS

---

COMPANY

---

CONNECT WITH US

