Security Advisory

AI Recommended Content

K000150668: TMM vulnerability CVE-2025-41431

Published Date: **May 7, 2025** **Updated Date:** **May 8, 2025**

Evaluated products:

Security Advisory Description

When connection mirroring is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate in the standby BIG-IP systems in a traffic group. (CVE-2025-41431)

Impact

Traffic in other traffic groups may be disrupted while the TMM process restarts on the standby systems. This vulnerability allows a remote, unauthenticated attacker to cause a denial-of-service (DoS) on the standby BIG-IP systems in a traffic group, temporarily reducing the redundancy in a BIG-IP cluster while the standby systems restart. There is no control plane exposure; this is a data plane issue only.

Security Advisory Status

F5 Product Development has assigned ID 1783221 (BIG-IP) to this vulnerability. This issue has been classified as CWE-787: Out-of-bounds Write.

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

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[1]	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

[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 (all modules)	17.x	17.1.2	17.1.2.2	**High/7.5** (CVSS v3.1) **High/8.7** (CVSS v4.0)	TMM
	16.x	None	Not applicable		
	15.x	None	Not applicable		
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.

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

[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.

Mitigation

To mitigate this vulnerability for the BIG-IP system, you can set the **statemirror.verify** database variable value to **enable**. To do so, perform the following procedure:

Impact of action: *Performing the following procedure should not have a negative impact on your system.*

1. Log in to the Advanced Shell (**bash**).
2. Set the **statemirror.verify** database variable value to **enable** by entering the following command:

   ```
   tmsh modify /sys db statemirror.verify value enable
   ```
3. To verify the change, enter the following command:

   ```
   tmsh list /sys db statemirror.verify all-properties
   ```

   Output should appear similar to the following example:

   ```
   sys db statemirror.verify {
       default-value "disable"
       scf-config "true"
       value "enable"
       value-range "disable enable"
   }
   ```

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)
- 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
- K000135931: Contact F5 Support

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