

[SIGN IN](#)

 Security Advisory



 [AI Recommended Content](#)

K000139503: F5OS vulnerability CVE-2025-46265

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

✓ Evaluated products:

Final- This article is marked as 'Final' because the security issue described in this article either affected F5 products at one time and was resolved or it never affected F5 products. Unless new information is discovered, F5 will no longer update the article.

Security Advisory Description

On F5OS, an improper authorization vulnerability exists where remotely authenticated users (LDAP, RADIUS, TACACS+) may be authorized with higher privilege F5OS roles. ([CVE-2025-46265](#))

Impact

This vulnerability may allow a remote, authenticated attacker to be unexpectedly granted higher privilege (example: F5OS admin role) in the F5OS system. This is a control plane issue; there is no data plane exposure.

Security Advisory Status

F5 Product Development has assigned ID 1388477 (F5OS-A and F5OS-C) to this vulnerability. This issue has been classified as **CWE-863: Incorrect Authorization**.

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 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 |

¹F5 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 171.2.1, the fix also applies to 171.2.2 and all later 171.x releases (171.3.x, 171.4.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 | Vulnerable component or feature |
|-------------------------------|--------|--|---------------------|---------------------|---------------------------------|
| BIG-IP (all modules) | All | None | Not applicable | Not vulnerable | None |
| BIG-IQ Centralized Management | All | None | Not applicable | Not vulnerable | None |

¹F5 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](#).

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 ² | Vulnerable component or feature |
|---------|--------|--|---------------------|--|---------------------------------|
| F5OS-A | 1.x | 1.5.1 | 1.8.0 1.5.2 | High/8.8 (CVSS v3.1) High/8.7 (CVSS v4.0) | ConfD |
| F5OS-C | 1.x | 1.6.0 - 1.6.2 | 1.8.0 | High/8.8 (CVSS v3.1) High/8.7 (CVSS v4.0) | ConfD |

¹F5 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](#).

²Starting 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](#).

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 |

¹F5 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 |
|---------|--------|--|---------------------|---------------------|---------------------------------|
|---------|--------|--|---------------------|---------------------|---------------------------------|

| | | | | | |
|-------------|-----|------|----------------|----------------|------|
| Traffic 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, in the remote authentication directory itself, do not assign any of the group IDs (GIDs) that F5OS defines (9000, 9001, and so on) to any groups. For a list of those GIDs, refer to the **Authentication & Access** chapter of the **F5 rSeries Systems** or the **F5 VELOS Systems: Administration and Configuration** manual.

Note: *For information about how to locate F5 product manuals, refer to [K98133564: Tips for searching MyF5 and finding product documentation](#).*

To review the role GIDs on F5OS, enter the following command in the F5OS command line:

```
show system aaa authentication roles role
```

Acknowledgments

This issue was discovered internally by F5.

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](#)
- [K21501912: Software lifecycle policy for F5OS](#)
- [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](#)
- [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](#)

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

[CONTACT SUPPORT](#)





[Trademarks](#)

[Policies](#)

[Privacy](#)

[California Privacy](#)

[Do Not Sell My Personal Information](#)