



# BIG-IP BFD vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2026-34019                                                                                                              |
| <b>State</b>           | PUBLISHED                                                                                                                   |
| <b>Assigner</b>        | f5                                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2026-05-13 16:16:39 UTC                                                                                                     |
| <b>Updated</b>         | 2026-05-13 16:27:11 UTC                                                                                                     |
| <b>Description</b>     | When Bidirectional Forwarding Detection (BFD) is configured in Static and Dynamic routing protocols, undisclosed traffic ca |

## Risk And Classification

**Primary CVSS:** v4.0 6.3 MEDIUM from f5sirt@f5.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000700000 probability, percentile 0.213440000 (date 2026-05-16)

**Problem Types:** CWE-410 | CWE-410 CWE-410: Insufficient Resource Pool

| Version | Source        | Type      | Score | Severity | Vector                                                                   |
|---------|---------------|-----------|-------|----------|--------------------------------------------------------------------------|
| 4.0     | f5sirt@f5.com | Secondary | 6.3   | MEDIUM   | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/C... |
| 4.0     | CNA           | CVSS      | 6.3   | MEDIUM   | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N          |
| 3.1     | f5sirt@f5.com | Primary   | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L                             |
| 3.1     | CNA           | CVSS      | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L                             |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

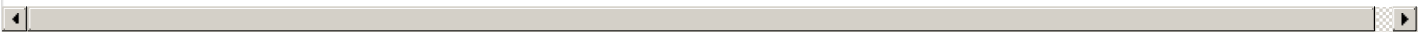
Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L



Vendor Declared Affected Products

| Source | Vendor | Product | Version                       | Platforms     |
|--------|--------|---------|-------------------------------|---------------|
| CNA    | F5     | BIG-IP  | unaffected 21.0.0 * custom    | Not specified |
| CNA    | F5     | BIG-IP  | affected 17.5.0 17.5.1 custom | Not specified |
| CNA    | F5     | BIG-IP  | affected 17.1.0 17.1.3 custom | Not specified |
| CNA    | F5     | BIG-IP  | affected 16.1.0 * custom      | Not specified |

| References                                                           |               |                                                 |                     |
|----------------------------------------------------------------------|---------------|-------------------------------------------------|---------------------|
| Reference                                                            | Source        | Link                                            | Tags                |
| my.f5.com/manage/s/article/K000150508                                | f5sirt@f5.com | <a href="https://my.f5.com">my.f5.com</a>       |                     |
| CVE Program record                                                   | CVE.ORG       | <a href="https://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail                                             | NVD           | <a href="https://nvd.nist.gov">nvd.nist.gov</a> | canonical, analysis |
| Vendor Comments And Credit                                           |               |                                                 |                     |
| Discovery Credit                                                     |               |                                                 |                     |
| <b>CNA: F5</b> (en)                                                  |               |                                                 |                     |
| There are currently no legacy QID mappings associated with this CVE. |               |                                                 |                     |

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)