



# CVE-2023-40534

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-40534
<b>State</b>	PUBLIC
<b>Assigner</b>	f5sirt@f5.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-10 13:15:00 UTC
<b>Updated</b>	2023-10-19 16:08:00 UTC
<b>Description</b>	When a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, and an iRule using the

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	17.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	17.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	17.1.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	17.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	17.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	17.1.0	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	17.1.0	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	17.1.0	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All

Application	F5	Big-ip Ddos Hybrid Defender	17.1.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	17.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	17.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	17.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	17.1.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	17.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	17.1.0	All	All	All
Application	F5	Big-ip Next Service Proxy For Kubernetes	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	17.1.0	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	17.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	17.1.0	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	17.1.0	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://my.f5.com/manage/s/article/K000133467">my.f5.com/manage/s/article/K000133467</a>	MISC	<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

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

378986 F5 BIG-IP Denial of Service (DoS) Vulnerability (K000133467)

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)