



# CVE-2023-24594

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

## Summary

<b>CVE</b>	CVE-2023-24594
<b>State</b>	PUBLIC
<b>Assigner</b>	f5sirt@f5.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-03 15:15:00 UTC
<b>Updated</b>	2023-10-05 14:59:00 UTC
<b>Description</b>	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	15.1.4.1	All	All	All
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	16.1.2	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	15.1.4.1	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	16.1.2	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	15.1.4.1	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	16.1.2	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	15.1.4.1	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	16.1.2	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	15.1.4.1	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	16.1.2	All	All	All
Application	F5	<a href="#">Big-ip Application Security Manager</a>	14.1.5	All	All	All
Application	F5	<a href="#">Big-ip Application Security Manager</a>	15.1.4.1	All	All	All

Application	F5	Big-ip Application Security Manager	16.1.2	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	14.1.5	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	15.1.4.1	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	16.1.2	All	All	All
Application	F5	Big-ip Carrier-grade Nat	14.1.5	All	All	All
Application	F5	Big-ip Carrier-grade Nat	15.1.4.1	All	All	All
Application	F5	Big-ip Carrier-grade Nat	16.1.2	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	14.1.5	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	15.1.4.1	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	16.1.2	All	All	All
Application	F5	Big-ip Domain Name System	14.1.5	All	All	All
Application	F5	Big-ip Domain Name System	15.1.4.1	All	All	All
Application	F5	Big-ip Domain Name System	16.1.2	All	All	All
Application	F5	Big-ip Edge Gateway	14.1.5	All	All	All
Application	F5	Big-ip Edge Gateway	15.1.4.1	All	All	All
Application	F5	Big-ip Edge Gateway	16.1.2	All	All	All
Application	F5	Big-ip Fraud Protection Service	14.1.5	All	All	All
Application	F5	Big-ip Fraud Protection Service	15.1.4.1	All	All	All
Application	F5	Big-ip Fraud Protection Service	16.1.2	All	All	All
Application	F5	Big-ip Global Traffic Manager	14.1.5	All	All	All
Application	F5	Big-ip Global Traffic Manager	15.1.4.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	16.1.2	All	All	All
Application	F5	Big-ip Link Controller	14.1.5	All	All	All
Application	F5	Big-ip Link Controller	15.1.4.1	All	All	All
Application	F5	Big-ip Link Controller	16.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	14.1.5	All	All	All
Application	F5	Big-ip Local Traffic Manager	15.1.4.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	16.1.2	All	All	All
Application	F5	Big-ip Next Service Proxy For Kubernetes	1.5.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	14.1.5	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	15.1.4.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	16.1.2	All	All	All
Application	F5	Big-ip Ssl Orchestrator	14.1.5	All	All	All
Application	F5	Big-ip Ssl Orchestrator	15.1.4.1	All	All	All
Application	F5	Big-ip Ssl Orchestrator	16.1.2	All	All	All

Application	F5	Big-ip Webaccelerator	14.1.5	All	All	All
Application	F5	Big-ip Webaccelerator	15.1.4.1	All	All	All
Application	F5	Big-ip Webaccelerator	16.1.2	All	All	All
Application	F5	Big-ip Websafe	14.1.5	All	All	All
Application	F5	Big-ip Websafe	15.1.4.1	All	All	All
Application	F5	Big-ip Websafe	16.1.2	All	All	All

## References

Reference	Source	Link	Tags
myF5	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

378486 F5 BIG-IP Traffic Management Microkernel (TMM) Vulnerability (K000133132)

© [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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

**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)