



# CVE-2021-22991

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-22991
<b>State</b>	PUBLIC
<b>Assigner</b>	f5sirt@f5.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-31 18:15:00 UTC
<b>Updated</b>	2023-08-08 14:21:00 UTC
<b>Description</b>	On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.3.6

## Risk And Classification

**EPSS:** 0.730950000 probability, percentile 0.987750000 (date 2026-04-02)

**CISA KEV:** Listed on 2022-01-18; due 2022-02-01; ransomware use Unknown

**Problem Types:** CWE-119

## CISA Known Exploited Vulnerability

<b>Vendor</b>	F5
<b>Product</b>	BIG-IP Traffic Management Microkernel
<b>Name</b>	F5 BIG-IP Traffic Management Microkernel Buffer Overflow
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-22991">https://nvd.nist.gov/vuln/detail/CVE-2021-22991</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Security Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Ddos Hybrid Defender</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Domain Name System</a>	All	All	All	All

Application	F5	<a href="#">Big-ip Fraud Protection Service</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Global Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Link Controller</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Local Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Policy Enforcement Manager</a>	All	All	All	All
Application	F5	<a href="#">Ssl Orchestrator</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://support.f5.com/csp/article/K56715231">support.f5.com/csp/article/K56715231</a>	MISC	<a href="https://support.f5.com">support.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
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[375749](#) F5 BIG-IP ASM,LTM,APM BIG-IP Traffic Management Microkernel (TMM) Buffer Overflow Vulnerability (K56715231)

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

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