# CVE Detail – CVE-2021-22991

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 12.1.5.3, undisclosed requests to a virtual server may be incorrectly handled by the Traffic Management Microkernel (TMM) URI normalization, which may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may theoretically allow bypass of URL based access control or remote code execution (RCE). Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.98612

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-100: Overflow Buffers
* CAPEC-123: Buffer Manipulation
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-42: MIME Conversion
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities

## Affected Products

* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_access\_policy\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_firewall\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_analytics:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_acceleration\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_application\_security\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_ddos\_hybrid\_defender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_domain\_name\_system:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_fraud\_protection\_service:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_global\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_link\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_local\_traffic\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:big-ip\_policy\_enforcement\_manager:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:f5:ssl\_orchestrator:\*:\*:\*:\*:\*:\*:\*:\*