



CVE-2022-28701

Published on: Not Yet Published

Last Modified on: 05/12/2022 04:23:00 PM UTC

CVE-2022-28701

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Big-ip Access Policy Manager](#) from [F5](#) contain the following vulnerability:

On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

CVE-2022-28701 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	support.f5.com text/html	MISC support.f5.com/csp/article/K99123750

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[376628](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Stream Profile Vulnerability (K99123750)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	16.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	16.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	16.1.2	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	16.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	16.1.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	16.1.2	All	All	All
Application	F5	Big-ip Analytics	16.1.0	All	All	All
Application	F5	Big-ip Analytics	16.1.1	All	All	All
Application	F5	Big-ip Analytics	16.1.2	All	All	All
Application	F5	Big-ip Application Acceleration Manager	16.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	16.1.1	All	All	All
Application	F5	Big-ip Application Acceleration Manager	16.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.2	All	All	All
Application	F5	Big-ip Domain Name System	16.1.0	All	All	All
Application	F5	Big-ip Domain Name System	16.1.1	All	All	All
Application	F5	Big-ip Domain Name System	16.1.2	All	All	All
Application	F5	Big-ip Domain Name System	17.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	16.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	16.1.1	All	All	All
Application	F5	Big-ip Fraud Protection Service	16.1.2	All	All	All
Application	F5	Big-ip Global Traffic Manager	16.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	16.1.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	16.1.2	All	All	All
Application	F5	Big-ip Link Controller	16.1.0	All	All	All
Application	F5	Big-ip Link Controller	16.1.1	All	All	All
Application	F5	Big-ip Link Controller	16.1.2	All	All	All

Application	F5	Big-ip Link Controller	16.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	16.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	16.1.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	16.1.2	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	16.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	16.1.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	16.1.2	All	All	All
cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_analytics:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_analytics:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_analytics:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_application_security_manager:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_application_security_manager:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_application_security_manager:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_domain_name_system:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_domain_name_system:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_domain_name_system:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_domain_name_system:17.0.0:*****:***:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:16.1.0:*****:***:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:16.1.1:*****:***:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:16.1.2:*****:***:						
cpe:2.3:a:f5:big-ip_global_traffic_manager:16.1.0:*****:***:						

cpe:2.3:a:f5:big-ip_global_traffic_manager:16.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_global_traffic_manager:16.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:16.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:16.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:16.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:16.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:16.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:16.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:16.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:16.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:16.1.2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-28701 : On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, when the stream profile is configured on a virtual... twitter.com/i/web/status/1...	2022-05-05 17:17:19
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-06 14:11:01
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-09 13:34:10
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-11 16:42:45
← Previous ID Next ID→		