



CVE-2021-23026

Published on: 09/14/2021 12:00:00 AM UTC

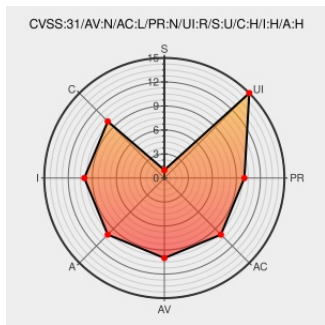
Last Modified on: 09/29/2021 07:21:00 PM UTC

CVE-2021-23026

Source: Mitre

Source: Nist

Print: PDF



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

BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x and 11.6.x and all versions of BIG-IQ 8.x, 7.x, and 6.x are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP.

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

CVE-2021-23026 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
No Description Provided	support.f5.com text/html	MISC support.f5.com/csp/article/K53854428

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

[375881](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) iControl SOAP Vulnerability (K53854428)

Exploit/POC from Github

PoC for exploiting CVE-2021-23026 : BIG-IP version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.4...

Known Affected Configurations (CPE V2.3)

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	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All

Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Centralized Management	All	All	All	All

Application	F5	Big-ip Centralized Management	All	All	All	All
Application	F5	Big-ip Centralized Management	All	All	All	All
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_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_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_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_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_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_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_ssl_orchestrator:~::~~::~~::~~::~~:::

cpe:2.3:a:f5:big-ip_ssl_orchestrator:~::~~::~~::~~::~~:::

cpe:2.3:a:f5:big-ip_ssl_orchestrator:~::~~::~~::~~::~~:::

cpe:2.3:a:f5:big-ip_ssl_orchestrator:*:*:*:*:*:*:

cpe:2.3:a:f5:big-iq_centralized_management:*:*:*:*:*:*:

cpe:2.3:a:f5:big-iq_centralized_management:*:*:*:*:*:*:

cpe:2.3:a:f5:big-iq_centralized_management:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2021 [Twitter](#) [LinkedIn](#) |

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](#)