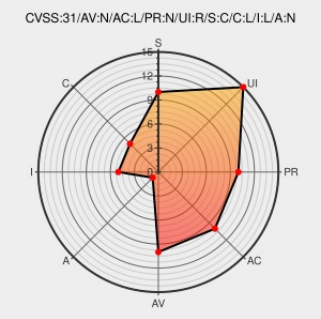
CVE-2021-23027

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

Last Modified on: 09/28/2021 06:51:00 PM UTC

CVE-2021-23027

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Big-ip Access Policy Manager from F5 contain the following vulnerability:

On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, and 14.1.x before 14.1.4.3, a DOM based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

CVE-2021-23027 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	support.f5.com text/html	MISC support.f5.com/csp/article/K24301698

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

375889 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Traffic Management User Interface (TMUI) Cross-Site Scripting (XSS) Vulnerability (K24301698)

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 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 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 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 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 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 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 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

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_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_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_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_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_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_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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@softek_jp	F5 Networks BIG-IP の TMUI の処理にクロスサイトスクリプティングの問題 (CVE-2021-23027) [39836] sid.softek.jp/content/show/3… #SIDfm #脆弱性情報	2021-08-27 09:12:57
@CVEreport	CVE-2021-23027 : On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3.1, and 14.1.x before 14.1.4.3, a DOM based… twitter.com/i/web/status/1…	2021-09-14 22:03:47
@0_exploit	CVE-2021-23027 dlvr.it/S7cFVr	2021-09-15 11:05:32

← Previous ID

Next ID→