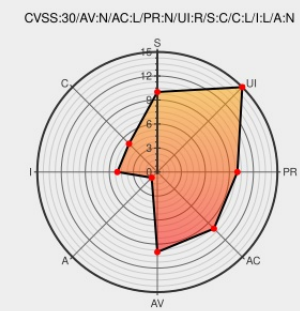
CVE-2018-15312

Published on: 10/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15312

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 13.0.0-13.1.1.1 and 12.1.0-12.1.3.6, a reflected Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an authenticated user to execute JavaScript for the currently logged-in user.

CVE-2018-15312 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **F5 Networks, Inc.** - **BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator)** version **13.0.0-13.1.1.1**

Affected Vendor/Software: **F5 Networks, Inc.** - **BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator)** version **12.1.0-12.1.3.6**

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
F5 BIG-IP Input Validation Flaw in Configuration Utility Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041932
No Description Provided	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K44462254

There are currently no QIDs associated with this CVE

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 Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	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 Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	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 Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	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 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 Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	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_advanced_firewall_manager:*:*:*:*:*:*:*:*:

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

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_security_manager:*:*:*:*:*:*:*:*:

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

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_edge_gateway:*:*:*:*:*:*:*:*:

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

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_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_policy_enforcement_manager:*:*:*:*:*:*:*:*:

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→