



# CVE-2021-23038

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

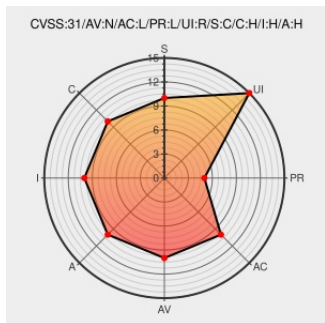
Last Modified on: 09/27/2021 03:43:00 PM UTC

## CVE-2021-23038

[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, 14.1.x before 14.1.4.2, 13.1.x before 13.1.4.1, and all versions of 12.1.x, a stored 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-2021-23038 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>SINGLE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
<b>No Description Provided</b>	<a href="#">support.f5.com</a> <a href="#">text/html</a>	<a href="#">MISC support.f5.com/csp/article/K61643620</a>

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](mailto:comment@cve.report).

## Related QID Numbers

[375903](#) 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 (K61643620)

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Access Policy Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Firewall Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Analytics</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Acceleration Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Security Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Application Security Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Domain Name System</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Domain Name System</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Fraud Protection Service</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Fraud Protection Service</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Global Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Global Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Link Controller</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Link Controller</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Local Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Local Traffic Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Policy Enforcement Manager</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Policy Enforcement Manager</a>	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_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:*.***:*.***:*.***:

No vendor comments have been submitted for this CVE

### Social Mentions

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

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**