



# CVE-2022-23026

Published on: 01/25/2022 12:00:00 AM UTC

Last Modified on: 02/01/2022 05:29:00 PM UTC

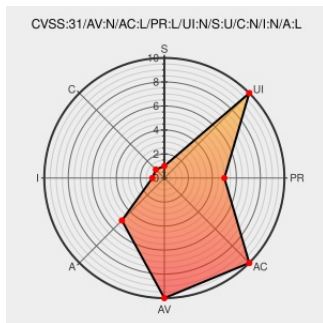
## CVE-2022-23026

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Big-ip Advanced Web Application Firewall](#) from F5 contain the following vulnerability:

On BIG-IP ASM & Advanced WAF version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.5, and all versions of 13.1.x and 12.1.x, an authenticated user with low privileges, such as a guest, can upload data using an undisclosed REST endpoint causing an increase in disk resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

CVE-2022-23026 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>NONE</b>	<b>LOW</b>

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>NONE</b>	<b>PARTIAL</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/K08402414</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

[376285](#) F5 BIG-IP Application Security Manager (ASM) and Advanced Web Application Firewall (WAF) REST API endpoint Vulnerability (K08402414)

[376291](#) F5 BIG-IP Application Security Manager (ASM) and Advanced Web Application Firewall (WAF) REST API endpoint Vulnerability (K08402414)

[376321](#) F5 BIG-IP Application Security Manager (ASM) and Advanced Web Application Firewall (WAF) REST API endpoint Vulnerability (K08402414)

[376343](#) F5 BIG-IP Application Security Manager (ASM) and Advanced Web Application Firewall (WAF) REST API endpoint Vulnerability (K08402414)

[376359](#) F5 BIG-IP Application Security Manager (ASM) and Advanced Web Application Firewall (WAF) REST API endpoint Vulnerability (K08402414)

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</a>	All	All	All	All
Application	F5	<a href="#">Big-ip Advanced Web Application Firewall</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 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 Acceleration Manager</a>	All	All	All	All

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\_advanced\_web\_application\_firewall:\*:\*:\*:\*:\*:

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_acceleration_manager:****:*:*:*:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:****:*:*:*:



No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @SombbreroBlanc0	K08402414: BIG-IP ASM and Advanced WAF REST API endpoint vulnerability CVE-2022-23026 <a href="https://ccn-cert.cni.es/component/vuln...">ccn-cert.cni.es/component/vuln...</a>	2022-01-20 10:37:28
 @softtek_jp	F5 Networks BIG-IP ASM, Advanced WAF に設定ユーティリティを機能しなくされる問題 (CVE-2022-23026) [41103] <a href="https://sid.softtek.jp/content/show/4...">sid.softtek.jp/content/show/4...</a> #SIDfm #脆弱性情報	2022-01-21 06:34:22
 @CVEreport	CVE-2022-23026 : On BIG-IP ASM & Advanced WAF version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 1... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-01-25 20:12:53
 /r/netcve	<a href="#">CVE-2022-23026</a>	2022-01-25 21:39:07

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |  
 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](#)**