



CVE-2021-23028

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

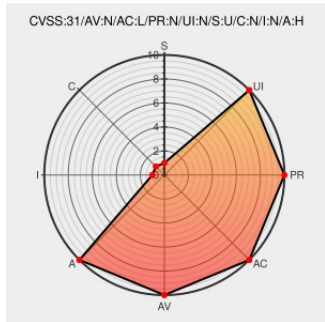
Last Modified on: 09/24/2021 07:19:00 PM UTC

CVE-2021-23028

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Big-ip Advanced Web Application Firewall](#) 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, and 13.1.x before 13.1.4, when JSON content profiles are configured for URLs as part of an F5 Advanced Web Application Firewall (WAF)/BIG-IP ASM security policy and applied to a virtual server, undisclosed requests may cause the BIG-IP ASM bd process to

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

CVE-2021-23028 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
NVD Description	CVE-2021-23028	MISC support.f5.com/doc/article/K00600025

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

375894 F5 BIG-IP Application Security Manager (ASM) Denial of Service (DoS) Vulnerability (K00602225)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	16.0.1	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 Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	16.0.1	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

`cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:*:*:*:*:*:*:`

`cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:16.0.1:*:*:*:*:*:`

`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_security_manager:*:*:*:*:*:*:`

`cpe:2.3:a:f5:big-ip_application_security_manager:16.0.1:*:*:*:*:*:`

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

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

No vendor comments have been submitted for this CVE

Social Mentions

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

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#)