



CVE-2017-0302

Published on: 05/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:51 PM UTC

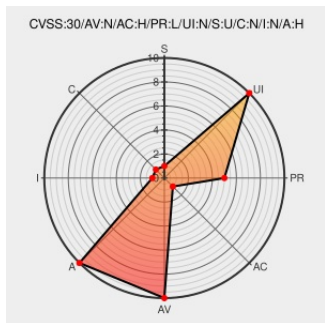
CVE-2017-0302

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Big-ip Access Policy Manager](#) from [F5](#) contain the following vulnerability:

In F5 BIG-IP APM 12.0.0 through 12.1.2 and 13.0.0, an authenticated user with an established access session to the BIG-IP APM system may be able to cause a traffic disruption if the length of the requested URL is less than 16 characters.

CVE-2017-0302 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP APM version 13.0.0**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP APM version 12.0.0 - 12.1.2**

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
-------------	------	------

F5 BIG-IP APM 12.0.0 through 12.1.2 and 13.0.0, an authenticated user with an established access session to the BIG-IP APM system may be able to cause a traffic disruption if the length of the requested URL is less than 16 characters. [CVE-2017-0302](#)

F5 BIG-IP APM URL Validation Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker

[www.securitytracker.com](https://www.securitytracker.com/text/html)
text/html

SEC TRACK 1038408

No Description Provided

Vendor Advisory
[support.f5.com](https://support.f5.com/text/html)
text/html

CONFIRM
support.f5.com/csp/article/K87141725

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.

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	12.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
cpe:2.3:a:f5:big-ip_access_policy_manager:12.0.0:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.0:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.1:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.2:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:13.0.0:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.0.0:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.0:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.1:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.2:****:****:.						
cpe:2.3:a:f5:big-ip_access_policy_manager:13.0.0:****:****:.						

No vendor comments have been submitted for this CVE

© [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](#)