



CVE-2018-5517

Published on: 05/02/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

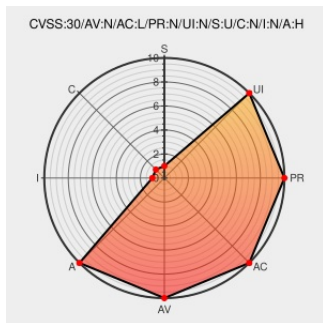
CVE-2018-5517

[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 13.1.0-13.1.0.5, malformed TCP packets sent to a self IP address or a FastL4 virtual server may cause an interruption of service. The control plane is not exposed to this issue. This issue impacts the data plane virtual servers and self IPs.

CVE-2018-5517 has been assigned by [f5sirt@f5.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [F5 Networks, Inc.](#) - **BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe)** version **13.1.0-13.1.0.5**

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: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
F5 BIG-IP TCP Processing Flaw in the TMM Kernel Lets Remote Users Deny Data Plane Service - SecurityTracker	Third Party Advisory VDB Entry	SECTrack 1040805

Vendor Advisory
support.f5.com
text/html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
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 Analytics	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 Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	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 Local Traffic 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 Websafe	All	All	All	All

```
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_policy_enforcement_manager:*.*.*.*.*.*.*.*:
cpe:2.3:a:f5:big-ip_webaccelerator:*.*.*.*.*.*.*.*:
cpe:2.3:a:f5:big-ip_websafe:*.*.*.*.*.*.*.*:

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_webaccelerator:*.*.*.*.*.*.*.*:
cpe:2.3:a:f5:big-ip_websafe:*.*.*.*.*.*.*.*:

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_webaccelerator:*.*.*.*.*.*.*.*:
cpe:2.3:a:f5:big-ip_websafe:*.*.*.*.*.*.*.*:

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_webaccelerator:*.*.*.*.*.*.*.*:
cpe:2.3:a:f5:big-ip_websafe:*.*.*.*.*.*.*.*:

No vendor comments have been submitted for this CVE

[← 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