



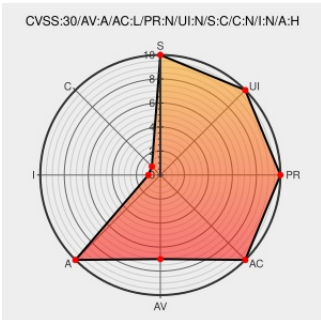
Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5531

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Through undisclosed methods, on F5 BIG-IP 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.0-11.6.3.1, or 11.2.1-11.5.6, adjacent network attackers can cause a denial of service for VCMF guest and host systems. Attack must be sourced from adjacent network (layer 2).

CVE-2018-5531 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, FPS, GTM, Link Controller, PEM, WebAccelerator)** version 13.0.0-13.1.0.7

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) version 12.1.0-12.1.3.5**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator)** version 11.6.0-11.6.3.1

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) version 11.2.1-11.5.6**

CVSS3 Score: 7.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 6.1 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	Mitigation Vendor Advisory support.f5.com text/html	 CONFIRM support.f5.com/csp/article/K64721111

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	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
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 Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall 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 Analytics	All	All	All	All
Application	F5	Big-ip Analytics	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 Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	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 Application Security Manager	All	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
Application	F5	Big-ip Domain Name System	All	All	All	All

Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	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 Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	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 Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	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 Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	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 Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement 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 Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	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_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_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_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_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_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_domain_name_system:*:*:*:*:*:*
```

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

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

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

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

```
cpe:2.3:a:f5:big-ip edge_gateway:*.~*~*~*~*~*~*~*~*~*
```

```
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_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_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_link_controller:*****:
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_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:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_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_webaccelerator:*****:
cpe:2.3:a:f5:big-ip_webaccelerator:*****:
cpe:2.3:a:f5:big-ip_webaccelerator:*****:

No vendor comments have been submitted for this CVE

