



CVE-2018-5527

Published on: 06/27/2018 12:00:00 AM UTC

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

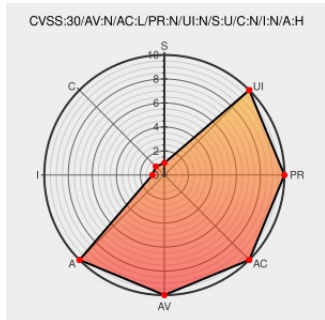
CVE-2018-5527

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

On BIG-IP 13.1.0-13.1.0.7, a remote attacker using undisclosed methods against virtual servers configured with a Client SSL or Server SSL profile that has the SSL Forward Proxy feature enabled can force the Traffic Management Microkernel (tmk) to leak memory. As a result, system memory usage increases over time, which may eventually cause a decrease in performance or a system reboot due to memory exhaustion.

CVE-2018-5527 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..7

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: **7.8 - HIGH**

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

CVE References

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

Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	 CONFIRM support.f5.com/csp/article/K20134942
F5 BIG-IP SSL Forward Proxy Flaw Lets Remote Users Consume Excessive Memory Resources - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1041196

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 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 access policy 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_application_acceleration_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 edge gateway:*:*:*:*:*:
```

```
ospf0-0>show ip ospf database
```

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_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 →](#)