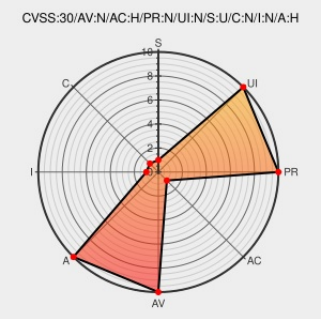
CVE-2017-6141

Published on: 10/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:49 PM UTC

CVE-2017-6141

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 LTM, AAM, AFM, APM, ASM, Link Controller, PEM, and WebSafe 12.1.0 through 12.1.2, certain values in a TLS abbreviated handshake when using a client SSL profile with the Session Ticket option enabled may cause disruption of service to the Traffic Management Microkernel (TMM). The Session Ticket option is disabled by default.

CVE-2017-6141 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **F5 Networks, Inc.** - **F5 BIG-IP LTM, AAM, AFM, APM, ASM, Link Controller, PEM, WebSafe** version **12.1.0 through 12.1.2**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	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

Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K21154730

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	12.1.0	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	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 Advanced Firewall Manager	12.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.2	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.2	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.1	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.2	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.1	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.2	All	All	All
Application	F5	Big-ip Link Controller	12.1.0	All	All	All

Application	F5	Big-ip Link Controller	12.1.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.2	All	All	All
Application	F5	Big-ip Link Controller	12.1.0	All	All	All
Application	F5	Big-ip Link Controller	12.1.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.2	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.2	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.2	All	All	All
Application	F5	Big-ip Websafe	12.1.0	All	All	All
Application	F5	Big-ip Websafe	12.1.1	All	All	All
Application	F5	Big-ip Websafe	12.1.2	All	All	All
Application	F5	Big-ip Websafe	12.1.0	All	All	All
Application	F5	Big-ip Websafe	12.1.1	All	All	All
Application	F5	Big-ip Websafe	12.1.2	All	All	All

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: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_advanced_firewall_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_link_controller:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→