

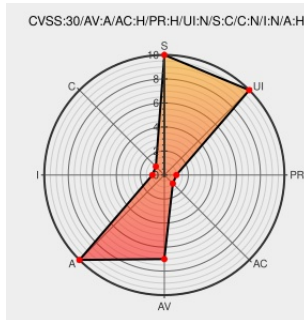


CVE-2018-5518

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

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-5518

[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 13.0.0-13.1.0.5 or 12.0.0-12.1.3.3, malicious root users with access to a VCMP guest can cause a disruption of service on adjacent VCMP guests running on the same host. Exploiting this vulnerability causes the vCMPd process on the adjacent VCMP guest to restart and produce a core file. This issue is only exploitable on a

VCMP guest which is operating in "host-only" or "bridged" mode. VCMP guests which are "isolated" are not impacted by this issue and do not provide mechanism to exploit the vulnerability. Guests which are deployed in "Appliance Mode" may be impacted however the exploit is not possible from an Appliance Mode guest. To exploit this vulnerability root access on a guest system deployed as "host-only" or "bridged" mode is required.

CVE-2018-5518 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **MEDIUM** 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 **13.0.0-13.1.0.5**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe)** version **12.0.0-12.1.3.3**

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **2.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
F5 BIG-IP vCMP Bug Lets Local Users on a Guest System Cause Denial of Service Conditions on Other Guest Systems - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1040797
No Description Provided	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K03165684

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 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 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 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 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

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_websafe:*****:
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