

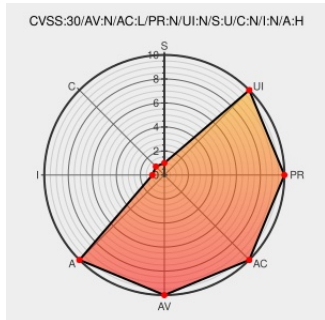


CVE-2018-5503

Published on: 03/22/2018 12:00:00 AM UTC

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

CVE-2018-5503

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

On F5 BIG-IP versions 13.0.0 - 13.1.0.3 or 12.0.0 - 12.1.3.1, TMM may restart when processing a specifically crafted page through a virtual server with an associated PEM policy that has content insertion as an action.

CVE-2018-5503 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (PEM)** version **13.0.0 - 13.1.0.3**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (PEM)** version **12.0.0 - 12.1.3.1**

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 13.0.0 - 13.1.0.3 or 12.0.0 - 12.1.3.1 TMM may restart when processing a specifically crafted page through a virtual server with an associated PEM policy that has content insertion as an action.	CVE-2018-5503	CVEPACK-1018503

F5 BIG-IP Policy Enforcement Manager (PEM) Content Insertion Bug
Lets Remote Users Deny Service - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

SEC TRACK 1040560

No Description Provided

Vendor Advisory

support.f5.com

text/html

CONFIRM

support.f5.com/csp/article/K54562183

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 Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →