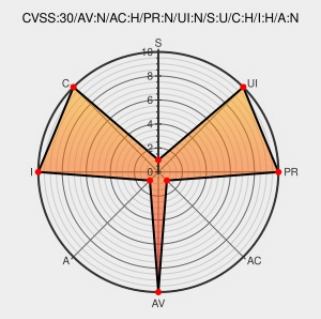
CVE-2017-6144

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

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6144

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Big-ip Policy Enforcement Manager from F5 contain the following vulnerability:

In F5 BIG-IP PEM 12.1.0 through 12.1.2 when downloading the Type Allocation Code (TAC) database file via HTTPS, the server's certificate is not verified. Attackers in a privileged network position may be able to launch a man-in-the-middle attack against these connections. TAC databases are used in BIG-IP PEM for Device Type and OS (DTOS) and Tethering detection. Customers not using BIG-IP PEM, not configuring downloads of TAC database files, or not using HTTP for that download are not affected.

CVE-2017-6144 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **F5 Networks, Inc.** - **F5 BIG-IP PEM** version **12.1.0 through 12.1.2**

CVSS3 Score: 7.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	Mitigation Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K81601350

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	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

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→