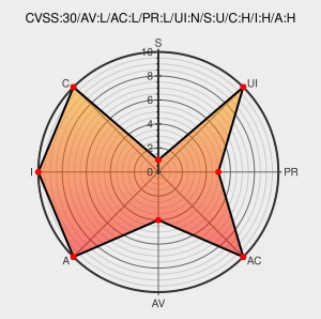
CVE-2018-5547

Published on: 08/17/2018 12:00:00 AM UTC

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

CVE-2018-5547

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



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

Windows Logon Integration feature of F5 BIG-IP APM client prior to version 7.1.7.1 for Windows by default uses Legacy logon mode which uses a SYSTEM account to establish network access. This feature displays a certificate user interface dialog box which contains the link to the certificate policy. By clicking on the link, unprivileged users can open additional dialog boxes and get access to the local machine windows explorer which can be used to get administrator privilege. Windows Logon Integration is vulnerable when the APM client is installed by an administrator on a user machine. Users accessing the local machine can get administrator privileges

CVE-2018-5547 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **F5 Networks, Inc.** - **BIG-IP APM client for Windows** version **Prior to version 7.1.7.1**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	support.f5.com text/html	CONFIRM support.f5.com/csp/article/K10015187?utm_source=f5support&utm_medium=RSS
F5 BIG-IP APM Client for Windows Lets Local Users Obtain System Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041511
No Description Provided	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/csp/article/K10015187

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 Client	7.1.6	All	All	All
Application	F5	Big-ip Access Policy Manager Client	7.1.6.1	All	All	All
Application	F5	Big-ip Access Policy Manager Client	7.1.7	All	All	All
Application	F5	Big-ip Access Policy Manager Client	7.1.6	All	All	All
Application	F5	Big-ip Access Policy Manager Client	7.1.6.1	All	All	All
Application	F5	Big-ip Access Policy Manager Client	7.1.7	All	All	All

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.7:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager_client:7.1.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report