



CVE-2018-5546

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-5546
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-17 12:29:00 UTC
Updated	2022-04-18 17:32:00 UTC
Description	The svpn and policyserver components of the F5 BIG-IP APM client prior to version 7.1.7.1 for Linux and macOS runs as a

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager Client	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

References

Reference	Source
support.f5.com/csp/article/K54431371	COM
security-research/CVE-2018-5529.txt at master · mirchr/security-research · GitHub	MIS
F5 BIG-IP APM Client for Linux/macOS 'svpn' and 'policyserver' Components Let Local Users Obtain Root Privileges - SecurityTracker	SEC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)