

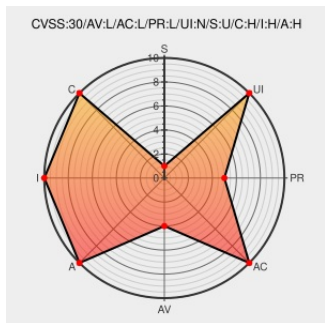


CVE-2019-12576

Published on: 07/11/2019 12:00:00 AM UTC

Last Modified on: 09/08/2021 05:22:00 PM UTC

CVE-2019-12576

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

Certain versions of [Macos](#) from [Apple](#) contain the following vulnerability:

A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The `openvpn_launcher` binary is setuid root. This program is called during the connection process and executes several operating system utilities to configure the system. The `networksetup` utility is called using relative paths. A local unprivileged user can execute arbitrary commands as root by creating a `networksetup` trojan which will be executed during the connection process. This is possible because the `PATH` environment variable is not reset prior to executing the OS utility.

CVE-2019-12576 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

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

security-research/CVE-2019-12576.txt at master · mirchr/security-research · GitHub

Tags

Exploit

Third Party Advisory

github.com

text/html

Link

 MISC github.com/mirchr/security-research/blob/master/vulnerabilities/PIA/CVE-2019-12576.txt

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
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Application	Londontrustmedia	Private Internet Access Vpn Client	82	All	All	All
Application	Londontrustmedia	Private Internet Access Vpn Client	82	All	All	All

cpe:2.3:o:apple:macos:-:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:

cpe:2.3:a:londontrustmedia:private_internet_access_vpn_client:82:*:*:*:*:*:

cpe:2.3:a:londontrustmedia:private_internet_access_vpn_client:82:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →