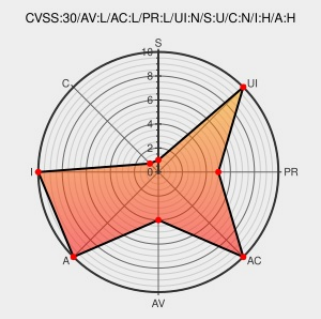
CVE-2019-12571

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

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

CVE-2019-12571

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 v0.9.8 beta (build 02099) for macOS could allow an authenticated, local attacker to overwrite arbitrary files. When the client initiates a connection, the XML /tmp/pia-watcher.plist file is created. If the file exists, it will be truncated and the contents completely overwritten. This file is removed on disconnect. An unprivileged user can create a hard or soft link to arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.

CVE-2019-12571 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 6.6 - MEDIUM

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

CVE References

Description	Tags	Link

security-research/CVE-2019-12571.txt at master · mirchr/security-research · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/mirchr/security-research/blob/master/vulnerabilities/PIA/CVE-2019-12571.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	0.9.8	beta	All	All
Application	Londontrustmedia	Private Internet Access Vpn Client	0.9.8	beta	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:0.9.8:beta:*:*:*:*:*:*:

cpe:2.3:a:londontrustmedia:private_internet_access_vpn_client:0.9.8:beta:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→