



CVE-2019-12578

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

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12578

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

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The `openvpn_launcher.64` binary is setuid root. This binary executes `/opt/pia/openvpn-64/openvpn`, passing the parameters provided from the command line.

Care was taken to programmatically disable potentially dangerous openvpn parameters; however, the `--route-pre-down` parameter can be used. This parameter accepts an arbitrary path to a script/program to be executed when OpenVPN exits. The `--script-security` parameter also needs to be passed to allow for this action to be taken, and `--script-security` is not currently in the disabled parameter list. A local unprivileged user can pass a malicious script/binary to the `--route-pre-down` option, which will be executed as root when openvpn is stopped.

CVE-2019-12578 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	Tags	Link
security-research/CVE-2019-12578.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-2019-12578.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	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	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:linux:linux_kernel:-:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

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→](#)

© CVE.report 2023   |

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](#)