

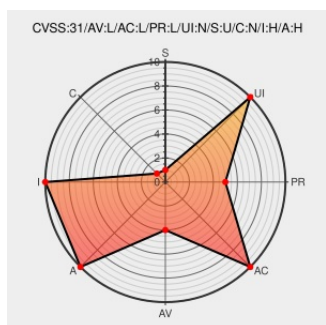


CVE-2019-16155

Published on: 02/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16155

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

Certain versions of [Forticlient](#) from [Fortinet](#) contain the following vulnerability:

A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctschd process. Further more, FortiClient for Linux 6.2.2 and below allow low

privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.

CVE-2019-16155 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiClientLinux** version **FortiClientLinux 6.2.1 and below**

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				
Multiple privilege escalations in FortiClient for Linux Danish Cyber Defence	Exploit Third Party Advisory danishcyberdefence.dk text/html	 MISC danishcyberdefence.dk/blog/forticlient_linux				
Privilege escalation and DoS in FortiClient for Linux through local IPC socket FortiGuard	Vendor Advisory fortiguard.com text/html	 CONFIRM fortiguard.com/psirt/FG-IR-19-238				
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
Application	Fortinet	Forticlient	All	All	All	All
cpe:2.3:a:fortinet:forticlient:*:*:*:*:linux:*:*						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID →		