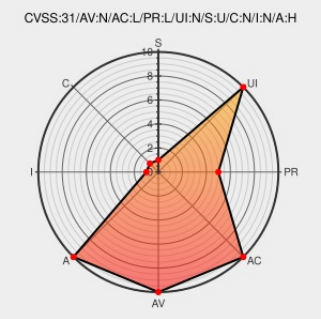
CVE-2019-17652

Published on: 02/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:38 PM UTC

CVE-2019-17652

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Forticlient from Fortinet contain the following vulnerability:

A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root priviledge crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctsched process due the argv data not been well sanitized.

CVE-2019-17652 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Multiple privilege escalations in FortiClient for Linux | Danish Cyber	Exploit	MISC

Defence	Third Party Advisory danishcyberdefence.dk text/html	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

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→