



# CVE-2019-11868

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-11868
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-29 17:15:00 UTC
<b>Updated</b>	2021-08-27 15:58:00 UTC
<b>Description</b>	See.sys, up to version 4.25, in SoftEther VPN Server versions 4.29 or older, allows a user to call an IOCTL specifying any k

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Softether	See.sys	All	All	All	All
Application	Softether	See.sys	All	All	All	All

## References

### Reference

DownWithUp's Github Website

2019/07/09: SE201901: SoftEther VPN Server NDIS 5.x Windows Local Bridge Driver Local Privilege Escalation Vulnerability - SoftEther VPN

SoftEtherVPN/src/See at master · SoftEtherVPN/SoftEtherVPN · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)