



# CVE-2017-7642

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-7642
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-02 19:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	The sudo helper in the HashiCorp Vagrant VMware Fusion plugin (aka vagrant-vmware-fusion) before 4.0.21 allows local u

## Risk And Classification

**Problem Types:** CWE-426

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashicorp	Vagrant Vmware Fusion	All	All	All	All

## References

Reference	Source	Link
Hashicorp vagrant-vmware-fusion < 4.0.20 - Local Privilege Escalation - macOS local Exploit	EXPLOIT-DB	<a href="#">www.exploit-db.com</a>
Full Disclosure: CVE-2017-7642 Local root privesc in Hashicorp vagrant-vmware-fusion <= 4.0.20	FULLDISC	<a href="#">seclists.org</a>
vagrant-plugin-changelog/vagrant-vmware-changelog.md at master · hashicorp/vagrant-plugin-changelog · GitHub	CONFIRM	<a href="#">github.com</a>
Mark Wadham	MISC	<a href="#">m4.rkw.io</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#).

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