



# CVE-2021-20078

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

## Summary

<b>CVE</b>	CVE-2021-20078
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnreport@tenable.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-01 19:15:00 UTC
<b>Updated</b>	2021-06-22 17:29:00 UTC
<b>Description</b>	Manage Engine OpManager builds below 125346 are vulnerable to a remote denial of service vulnerability due to a path tra

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	All	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125000	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125002	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125100	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125101	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125102	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125108	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125110	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125111	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125112	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125113	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125114	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125116	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125117	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125118	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125120	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Opmanager</a>	12.5	125121	All	All







Application	Zohocorp	Manageengine Opmanager	12.5	build125216	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125228	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125229	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125230	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125231	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125232	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125233	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125312	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125323	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125324	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125326	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125328	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125329	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125340	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125341	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125342	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125343	All	All
Application	Zohocorp	Manageengine Opmanager	12.5	build125344	All	All

## References

Reference	Source	Link	Tags
ManageEngine OpManager Remote Directory Deletion - Research Advisory   Tenable®	MISC	<a href="http://www.tenable.com">www.tenable.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)