



# CVE-2021-44525

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-44525
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-12-20 16:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	Zoho ManageEngine PAM360 before build 5303 allows attackers to modify a few aspects of application state because of a

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.0	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.0	build4001	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.0	build4002	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.1	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.1	build4100	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.1	build4101	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.5	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.5	build4500	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	4.5	build4501	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	build5000	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	build5001	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	build5002	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	build5003	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.0	build5004	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.1	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.1	build5100	All	All

Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.2	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.2	build5200	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.3	All	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.3	build5300	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.3	build5301	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Pam360</a>	5.3	build5302	All	All

## References

Reference	Source	Link	Tags
POPOP	CONFIRM	<a href="http://pitstop.manageengine.com">pitstop.manageengine.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](#) 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](#)