



CVE-2022-29081

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-29081 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-04-28 20:15:00 UTC |
| Updated | 2023-08-08 14:21:00 UTC |
| Description | Zoho ManageEngine Access Manager Plus before 4302, Password Manager Pro before 12007, and PAM360 before 5401 |

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|----------------------------------|---------|-----------|---------|----------|
| Application | Zohocorp | Manageengine Access Manager Plus | 4.0 | build4000 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.1 | build4100 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.1 | build4101 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.2 | build4200 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.2 | build4201 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.2 | build4202 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.2 | build4203 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.3 | build4300 | All | All |
| Application | Zohocorp | Manageengine Access Manager Plus | 4.3 | build4301 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.0 | build4001 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.0 | build4002 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.1 | build4100 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.1 | build4101 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.5 | build4500 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 4.5 | build4501 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.0 | build5000 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.0 | build5001 | All | All |

| | | | | | | |
|-------------|----------|-----------------------------------|------|-------------|-----|-----|
| Application | Zohocorp | Manageengine Pam360 | 5.0 | build5002 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.0 | build5003 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.0 | build5004 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.1 | build5100 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.2 | build5200 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.3 | build5300 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.3 | build5301 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.3 | build5302 | All | All |
| Application | Zohocorp | Manageengine Pam360 | 5.4 | build5400 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.1 | build10103 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.1 | build10104 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.2 | build10200 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.3 | build10300 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.3 | build10301 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.3 | build10302 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.4 | build10400 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.4 | build10401 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 10.4 | build10402 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.1 | 11104 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.1 | build_11101 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.1 | build_11102 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.1 | build_11103 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.2 | 11200 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.2 | 11201 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.3 | build11300 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 11.3 | build11301 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12000 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12001 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12002 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12003 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12004 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12005 | All | All |
| Application | Zohocorp | Manageengine Password Manager Pro | 12.0 | build12006 | All | All |

References

| Reference | Source | Link |
|--|---------|--|
| ManageEngine Access Manager Plus REST API Restriction Bypass - Research Advisory Tenable® | MISC | www.tenable.com |
| RESTAPI Restriction Bypass Vulnerability - CVE-2022-29081 - ManageEngine Access Manager Plus | MISC | www.manageengine.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](#).

CVE.report and Source URL Uptime Status status.cve.report