



# CVE-2022-42904

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

## Summary

<b>CVE</b>	CVE-2022-42904
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-18 21:15:00 UTC
<b>Updated</b>	2022-11-22 16:13:00 UTC
<b>Description</b>	Zoho ManageEngine ADManager Plus through 7151 allows authenticated admin users to execute the commands in proxy s

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zohocorp	Manageengine Admanager Plus	All	All	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	-	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7100	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7101	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7102	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7110	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7111	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7112	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7113	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7114	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7115	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7116	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7117	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7118	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7120	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7121	All	All
Application	Zohocorp	Manageengine Admanager Plus	7.1	7122	All	All

Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7123	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7124	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7125	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7126	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7130	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7131	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7140	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7141	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7150	All	All
Application	<a href="#">Zohocorp</a>	<a href="#">Manageengine Admanager Plus</a>	7.1	7151	All	All

## References

Reference	Source	Link	Tags
Mitigate authenticated RCE vulnerability in ADManager Plus	MISC	<a href="http://www.manageengine.com">www.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](#).

Free CVE JSON API [cve.report/api](http://cve.report/api)

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