



CVE-2020-11531

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

Summary

CVE	CVE-2020-11531
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-08 21:15:00 UTC
Updated	2020-05-18 12:15:00 UTC
Description	The DataEngine Xnode Server application in Zoho ManageEngine DataSecurity Plus prior to 6.0.1 does not validate the da

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zohocorp	Manageengine Adaudit Plus	All	All	All	All
Application	Zohocorp	Manageengine Adaudit Plus	All	All	All	All
Application	Zohocorp	Manageengine Datasecurity Plus	All	All	All	All
Application	Zohocorp	Manageengine Datasecurity Plus	All	All	All	All

References

Reference	Source	Link	Ta
POPOP	CONFIRM	pitstop.manageengine.com	
Full Disclosure: DataSecurity Plus Xnode Server - Remote Code Execution via Path Traversal	MISC	seclists.org	Ex
ManageEngine DataSecurity Plus Path Traversal / Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375418](#) Zoho ManageEngine DataSecurity Plus Remote Code Execution Vulnerability

© [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](#)