



CVE-2019-8928

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

Summary

CVE	CVE-2019-8928
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-17 15:29:00 UTC
Updated	2019-05-17 17:34:00 UTC
Description	An issue was discovered in Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2. XSS exists in /netflow/jspui/userMe

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zohocorp	Manageengine Netflow Analyzer	7.0.0.2	All	All	All
Application	Zohocorp	Manageengine Netflow Analyzer	7.0.0.2	All	All	All

References

Reference
Full Disclosure: [CVE-2019-8925 to CVE-2019-8929] Path traversal and Cross Site Scripting in Zoho ManageEngine Netflow Analyzer Profes
Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2 - Path Traversal / Cross-Site Scripting - JSP webapps Exploit
Real-Time NetFlow Analyzer NetFlow Traffic Analysis & Monitor Tool
Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2 Traversal / XSS ≈ Packet Storm
CVE Program record
NVD vulnerability detail

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](#)