

CVE-2022-47966

Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability

Exigent

CISA KEV since Jan 23, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Multiple Zoho ManageEngine on-premise products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of Apache Santuario xmlsec (aka XML Security for Java) 1.4.1, because the xmlsec XSLT features, by design in that version, make the application responsible for certain security protections, and the ManageEngine applications did not provide those protections.

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.998

99.95th percentile · FIRST

CISA DEADLINE

Feb 13, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

This affects Access Manager Plus before 4308, Active Directory 360 before 4310, ADAudit Plus before 7081, ADManager Plus before 7162, ADSelfService Plus before 6211, Analytics Plus before 5150, Application Control Plus before 10.1.2220.18, Asset Explorer before 6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11, Endpoint Central MSP before 10.1.2228.11, Endpoint DLP before 10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41. ServiceDesk Plus before 14004, ServiceDesk Plus MSP before 13001, SupportCenter Plus before 11026, and Vulnerability Manager Plus before 10.1.2220.18. Exploitation is only possible if SAML SSO has ever been configured for a product (for some products, exploitation requires that SAML SSO is currently active).

Affected and fixed versions · 14 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
manageengine access manager plus	< 4.3 4.3	4.3	NVD
manageengine ad360	< 4.3 4.3	4.3	NVD
manageengine adaudit plus	< 7.0 7.0	7.0	NVD
manageengine admanager plus	< 7.1 7.1	7.1	NVD
manageengine adselfservice plus	< 6.2 6.2	6.2	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
manageengine analytics plus	< 5.1 5.1	5.1	NVD
manageengine assetexplorer	< 6.9 6.9	no fixed version listed	NVD
manageengine key manager plus	< 6.4 6.4	no fixed version listed	NVD

Sources

Vendor guidance	manageengine.com/security/advisory/CVE/cve-2022-47966.html	NVD	nvd.nist.gov/vuln/detail/CVE-2022-47966
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-50684
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-47966		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.