

CVE-2021-44077

Zoho ManageEngine ServiceDesk Plus Remote Code Execution Vulnerability

Exigent CISA KEV since Dec 1, 2021 Actively exploited Public exploit module (Metasploit)

Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution. This is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.

EVRS 85 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.933 99.84th percentile · FIRST	CISA DEADLINE Dec 15, 2021 KEV since 2021 · 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.933 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
manageengine servicedesk plus	< 11.1 11.1 11.2 11.3	11.1	NVD
manageengine servicedesk plus msp	< 10.5 10.5	10.5	NVD
manageengine supportcenter plus	< 11.0 11.0	11.0	NVD

Sources

Vendor guidance	pitstop.manageengine.com/portal/en/community/topic/security-advisory-authentication-bypass-vulnerability-in-servicedesk-plus-versions-11138-and-above	NVD	nvd.nist.gov/vuln/detail/CVE-2021-44077
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-30936
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-44077		

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