

CVE-2019-8394

Zoho ManageEngine ServiceDesk Plus (SDP) File Upload Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Zoho ManageEngine ServiceDesk Plus (SDP) before 10.0 build 10012 allows remote attackers to upload arbitrary files via login page customization.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 6.5 Medium · NVD	EPSS 0.633 99.21st percentile · FIRST	CISA DEADLINE May 3, 2022 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	0.633 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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	< 10.0.0 10.0.0	10.0.0	NVD

Sources

Vendor guidance	manageengine.com/products/service-desk/readme.html	NVD	nvd.nist.gov/vuln/detail/CVE-2019-8394
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-17784
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-8394		

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