CVE-2020-10189

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10189
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-06 17:15:00 UTC
Updated	2022-10-07 13:42:00 UTC
Description	Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untruste

Risk And Classification

EPSS: 0.942480000 probability, percentile 0.999290000 (date 2026-04-02)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-502

CISA Known Exploited Vulnerability

Vendor	Zoho
Product	ManageEngine
Name	Zoho ManageEngine Desktop Central File Upload Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-10189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zohocorp	Manageengine Desktop Central	All	All	All	All
Application	Zohocorp	Manageengine Desktop Central	10	All	All	All
Application	Zohocorp	Manageengine Desktop Central	10	All	All	All

References

Reference	Source	Link	Tags
Source Incite	MISC	srcincite.io	Exploit, Third Party Adviso
srcincite.io/pocs/src-2020-0011.py.txt	MISC	srcincite.io	Exploit, Third Party Adviso

Remote Code Execution Vulnerability | ManageEngine Desktop Central	CONFIRM	www.manageengine.com	
ManageEngine Desktop Central Java Deserialization ≈ Packet Storm	MISC	packetstormsecurity.com	
Zoho zero-day published on Twitter | ZDNet	MISC	www.zdnet.com	Third Party Advisory
CWE - CWE-502: Deserialization of Untrusted Data (4.3)	MISC	cwe.mitre.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.