



# CVE-2020-10189

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

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

## 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

|                        |   |
|------------------------|---|
| <b>Vendor</b>          | Zoho  |
| <b>Product</b>         | ManageEngine  |
| <b>Name</b>            | Zoho ManageEngine Desktop Central File Upload Vulnerability   |
| <b>Required Action</b> | Apply updates per vendor instructions.  |
| <b>Notes</b>           | <a href="https://nvd.nist.gov/vuln/detail/CVE-2020-10189">https://nvd.nist.gov/vuln/detail/CVE-2020-10189</a> |

## 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   | <a href="https://srcincite.io">srcincite.io</a> | Exploit, Third Party Advisory |
| <a href="https://srcincite.io/pocs/src-2020-0011.py.txt">srcincite.io/pocs/src-2020-0011.py.txt</a> | MISC   | <a href="https://srcincite.io">srcincite.io</a> | Exploit, Third Party Advisory |

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

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)