



CVE-2026-34290

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-34290 |
| State | PUBLISHED |
| Assigner | oracle |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-21 21:16:33 UTC |
| Updated | 2026-04-22 14:16:56 UTC |
| Description | Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supp |

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert_us@oracle.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-400 | Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Identity Manager Connector. | CWE-400 CWE-400 Uncontrolled Resource Consumption

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|---|
| 3.1 | secalert_us@oracle.com | Secondary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1 | CNA | DECLARED | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------------------------------|---|----------------------------|---------------|
| CNA | Oracle Corporation | Oracle Identity Manager Connector | affected 12.2.1.4.0 semver | Not specified |

References

| Reference | Source | Link | Tags |
|--|--|--|---------------------|
| www.oracle.com/security-alerts/cpuapr2026.html | secalert_us@oracle.com | www.oracle.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report