



# CVE-2026-34284

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

## Summary

<b>CVE</b>	CVE-2026-34284
<b>State</b>	PUBLISHED
<b>Assigner</b>	oracle
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 21:16:32 UTC
<b>Updated</b>	2026-04-22 18:16:30 UTC
<b>Description</b>	Vulnerability in the Oracle Business Process Management Suite product of Oracle Fusion Middleware (component: Human

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from secalert\_us@oracle.com

**CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N**

**Problem Types:** CWE-284 | CWE-601 | Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Process Management Suite accessible data as well as unauthorized read access to a subset of Oracle Business Process Management Suite accessible data. | CWE-601 CWE-601 URL Redirection to Untrusted Site ('Open Redirect') | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Business Process Management Suite</a>	affected 12.2.1.4.0 semver	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Business Process Management Suite</a>	affected 14.1.2.0.0 semver	Not specified

#### References

Reference	Source	Link	Tags
<a href="http://www.oracle.com/security-alerts/cpuapr2026.html">www.oracle.com/security-alerts/cpuapr2026.html</a>	<a href="mailto:secalert_us@oracle.com">secalert_us@oracle.com</a>	<a href="http://www.oracle.com">www.oracle.com</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

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](https://cve.report/api)

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