CVE-2026-34302

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34302
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 21:16:35 UTC
Updated	2026-04-22 14:16:58 UTC
Description	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Loader). Supported versions

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from secalert_us@oracle.com

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

Problem Types: CWE-284 | Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Workflow. While the vulnerability is in Oracle Workflow, 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 Workflow accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Workflow. | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	5.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:L
3.1	CNA	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Oracle Workflow	affected 12.2.3 12.2.15 custom	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.