CVE-2015-4902

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

Summary

CVE	CVE-2015-4902
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-22 00:00:03 UTC
Updated	2026-04-22 13:04:08 UTC
Description	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60 allows remote attackers to affect integrity via unknown v

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ADP

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

EPSS: 0.076810000 probability, percentile 0.919230000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | CWE-284 | n/a | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

CISA Known Exploited Vulnerability

Vendor	Oracle
Product	Java SE
Name	Oracle Java SE Integrity Check Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-4902

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Oracle	Jdk	1.6.0	update101	All	All
Application	Oracle	Jdk	1.7.0	update85	All	All
Application	Oracle	Jdk	1.8.0	update60	All	All
Application	Oracle	Jre	1.6.0	update101	All	All

Application	Oracle	Jre	1.7.0	update85	All	All
Application	Oracle	Jre	1.8.0	update60	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.3	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	5.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	6.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	7.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	6.7_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.2_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.3_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.4_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.5_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	5.0_ppc	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	6.0_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	6.7_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.2_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.3_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.4_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.5_ppc64	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.2_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.3_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.4_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.5_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	6.0	All	All	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Satellite	5.6	All	All	All
Application	Redhat	Satellite	5.7	All	All	All
Application	Suse	Linux Enterprise Module For Legacy	12	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Red Hat Customer Portal
[security-announce] openSUSE-SU-2015:1905-1: important: Security update
[security-announce] SUSE-SU-2015:2268-1: important: Security update for
Oracle Java SE Multiple Flaws Let Local and Remote Users Gain Elevated Privileges and Remote Users Access and Modify Data and Deny S
[security-announce] SUSE-SU-2015:2182-1: important: Security update for
[security-announce] openSUSE-SU-2016:0270-1: critical: Security update f
Red Hat Customer Portal

Red Hat Customer Portal
Oracle Critical Patch Update - October 2015
[security-announce] SUSE-SU-2015:2168-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
Oracle Java SE CVE-2015-4902 Remote Security Vulnerability
Red Hat Customer Portal
Red Hat Customer Portal
[security-announce] SUSE-SU-2015:2166-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201603-11) — Gentoo Security
[security-announce] SUSE-SU-2015:2192-1: important: Security update for
[security-announce] SUSE-SU-2016:0113-1: important: Security update for
www.cisa.gov/known-exploited-vulnerabilities-catalog
[security-announce] SUSE-SU-2015:2216-1: important: Security update for
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-03T00:00:00.000Z	CVE-2015-4902 added to CISA KEV

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 registred 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**