CVE-2015-2590

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

Summary

CVE	CVE-2015-2590
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-16 10:59:17 UTC
Updated	2026-04-21 18:07:25 UTC
Description	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote a

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.611440000 probability, percentile 0.983230000 (date 2026-04-23)

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

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Oracle
Product	Java SE
Name	Oracle Java SE and Java SE Embedded Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-2590

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Oracle	Jdk	1.6.0	update95	All	All
Application	Oracle	Jdk	1.7.0	update75	All	All
Application	Oracle	Jdk	1.7.0	update80	All	All
Application	Oracle	Jdk	1.8.0	update33	All	All
Application	Oracle	Jdk	1.8.0	update45	All	All
Application	Oracle	Jre	1.6.0	update95	All	All
Application	Oracle	Jre	1.7.0	update75	All	All
Application	Oracle	Jre	1.7.0	update80	All	All
Application	Oracle	Jre	1.8.0	update33	All	All
Application	Oracle	Jre	1.8.0	update45	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	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.1	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 For Ibm Z Systems	6.0_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	7.1_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	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	7.1_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	7.1_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 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 Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	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 Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Server	12	-	All	All

Vendor Declared Affected Products

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

References

Reference
[security-announce] openSUSE-SU-2015:1289-1: important: Security update
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Oracle Critical Patch Update - July 2015
Debian -- Security Information -- DSA-3316-1 openjdk-7
[security-announce] openSUSE-SU-2015:1288-1: important: Security update
Red Hat Customer Portal
Oracle Java SE Multiple Flaws Lets Local and Remote Users Gain Elevated Privileges and Remote Users Partially Access Data, Modify Data,
Red Hat Customer Portal
Debian -- Security Information -- DSA-3339-1 openjdk-6
[security-announce] SUSE-SU-2015:1319-1: important: Security update for
Oracle Java SE CVE-2015-2590 Remote Security Vulnerability
[security-announce] SUSE-SU-2015:1320-1: important: Security update for
Red Hat Customer Portal
Red Hat Customer Portal
USN-2706-1: OpenJDK 6 vulnerabilities | Ubuntu
www.cisa.gov/known-exploited-vulnerabilities-catalog
IcedTea: Multiple vulnerabilities (GLSA 201603-14) — Gentoo security
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201603-11) — Gentoo Security
USN-2696-1: OpenJDK 7 vulnerabilities | Ubuntu
Red Hat Customer Portal
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-2015-2590 added to CISA KEV

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

Free CVE JSON API cve.report/api

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