



# CVE-2012-4681

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

## Summary

<b>CVE</b>	CVE-2012-4681
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-08-28 00:55:01 UTC
<b>Updated</b>	2026-04-21 18:38:11 UTC
<b>Description</b>	Multiple vulnerabilities in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier allow r

## 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:** 0.941400000 probability, percentile 0.999160000 (date 2026-04-25)

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

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

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

<b>Vendor</b>	Oracle
<b>Product</b>	Java SE
<b>Name</b>	Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2012-4681">https://nvd.nist.gov/vuln/detail/CVE-2012-4681</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Jdk	1.6.0	-	All	All
Application	Oracle	Jdk	1.6.0	update1	All	All
Application	Oracle	Jdk	1.6.0	update10	All	All
Application	Oracle	Jdk	1.6.0	update11	All	All
Application	Oracle	Jdk	1.6.0	update12	All	All

Application	Oracle	Jdk	1.6.0	update13	All	All
Application	Oracle	Jdk	1.6.0	update14	All	All
Application	Oracle	Jdk	1.6.0	update15	All	All
Application	Oracle	Jdk	1.6.0	update16	All	All
Application	Oracle	Jdk	1.6.0	update17	All	All
Application	Oracle	Jdk	1.6.0	update18	All	All
Application	Oracle	Jdk	1.6.0	update19	All	All
Application	Oracle	Jdk	1.6.0	update2	All	All
Application	Oracle	Jdk	1.6.0	update20	All	All
Application	Oracle	Jdk	1.6.0	update21	All	All
Application	Oracle	Jdk	1.6.0	update22	All	All
Application	Oracle	Jdk	1.6.0	update23	All	All
Application	Oracle	Jdk	1.6.0	update24	All	All
Application	Oracle	Jdk	1.6.0	update25	All	All
Application	Oracle	Jdk	1.6.0	update26	All	All
Application	Oracle	Jdk	1.6.0	update27	All	All
Application	Oracle	Jdk	1.6.0	update29	All	All
Application	Oracle	Jdk	1.6.0	update3	All	All
Application	Oracle	Jdk	1.6.0	update30	All	All
Application	Oracle	Jdk	1.6.0	update31	All	All
Application	Oracle	Jdk	1.6.0	update32	All	All
Application	Oracle	Jdk	1.6.0	update33	All	All
Application	Oracle	Jdk	1.6.0	update34	All	All
Application	Oracle	Jdk	1.6.0	update4	All	All
Application	Oracle	Jdk	1.6.0	update5	All	All
Application	Oracle	Jdk	1.6.0	update6	All	All
Application	Oracle	Jdk	1.6.0	update7	All	All
Application	Oracle	Jdk	1.6.0	update8	All	All
Application	Oracle	Jdk	1.6.0	update9	All	All
Application	Oracle	Jdk	1.7.0	-	All	All
Application	Oracle	Jdk	1.7.0	update1	All	All
Application	Oracle	Jdk	1.7.0	update2	All	All
Application	Oracle	Jdk	1.7.0	update3	All	All
Application	Oracle	Jdk	1.7.0	update4	All	All
Application	Oracle	Jdk	1.7.0	update5	All	All

Application	Oracle	Jdk	1.7.0	update6	All	All
Application	Oracle	Jre	1.6.0	-	All	All
Application	Oracle	Jre	1.6.0	update1	All	All
Application	Oracle	Jre	1.6.0	update10	All	All
Application	Oracle	Jre	1.6.0	update11	All	All
Application	Oracle	Jre	1.6.0	update12	All	All
Application	Oracle	Jre	1.6.0	update13	All	All
Application	Oracle	Jre	1.6.0	update14	All	All
Application	Oracle	Jre	1.6.0	update15	All	All
Application	Oracle	Jre	1.6.0	update16	All	All
Application	Oracle	Jre	1.6.0	update17	All	All
Application	Oracle	Jre	1.6.0	update18	All	All
Application	Oracle	Jre	1.6.0	update19	All	All
Application	Oracle	Jre	1.6.0	update2	All	All
Application	Oracle	Jre	1.6.0	update20	All	All
Application	Oracle	Jre	1.6.0	update21	All	All
Application	Oracle	Jre	1.6.0	update22	All	All
Application	Oracle	Jre	1.6.0	update23	All	All
Application	Oracle	Jre	1.6.0	update24	All	All
Application	Oracle	Jre	1.6.0	update25	All	All
Application	Oracle	Jre	1.6.0	update26	All	All
Application	Oracle	Jre	1.6.0	update27	All	All
Application	Oracle	Jre	1.6.0	update29	All	All
Application	Oracle	Jre	1.6.0	update3	All	All
Application	Oracle	Jre	1.6.0	update30	All	All
Application	Oracle	Jre	1.6.0	update31	All	All
Application	Oracle	Jre	1.6.0	update32	All	All
Application	Oracle	Jre	1.6.0	update33	All	All
Application	Oracle	Jre	1.6.0	update34	All	All
Application	Oracle	Jre	1.6.0	update4	All	All
Application	Oracle	Jre	1.6.0	update5	All	All
Application	Oracle	Jre	1.6.0	update6	All	All
Application	Oracle	Jre	1.6.0	update7	All	All
Application	Oracle	Jre	1.6.0	update9	All	All
Application	Oracle	Jre	1.7.0	-	All	All
Application	Oracle	Jre	1.7.0	update1	All	All

Application	Oracle	Jre	1.7.0	update1	All	All
Application	Oracle	Jre	1.7.0	update2	All	All
Application	Oracle	Jre	1.7.0	update3	All	All
Application	Oracle	Jre	1.7.0	update4	All	All
Application	Oracle	Jre	1.7.0	update5	All	All
Application	Oracle	Jre	1.7.0	update6	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

### Vendor Declared Affected Products

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

### References

Reference
New Java 0day exploited in the wild - Alienvault Labs
'[security bulletin] HPSBUX02824 SSRT100970 rev.1 - HP-UX Running Java, Remote Execution of Arbitrary' - MARC
Metasploit: Let's start the week with a new Jav...   SecurityStreet
Red Hat Customer Portal
Alert for CVE-2012-4681
Malware Intelligence Lab from FireEye - Research & Analysis of Zero-Day & Advanced Targeted Threats:Zero-Day Season is Not Over Yet
DeepEnd Research: CVE-2012-4681 Java 7 0-Day vulnerability analysis
About Secunia Research   Flexera
[security-announce] SUSE-SU-2012:1231-1: important: Security update for
Immunity Products: Java 0day analysis (CVE-2012-4681)
US-CERT Alert TA12-240A - Oracle Java 7 Security Manager Bypass Vulnerability
Oracle Java Runtime Environment Remote Code Execution Vulnerability
www.cisa.gov/known-exploited-vulnerabilities-catalog
[security-announce] SUSE-SU-2012:1398-1: 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-2012-4681 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 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](#)