

CVE-2012-0507

Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability

Exigent

CISA KEV since Mar 3, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and 5.0 Update 33 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Concurrency. NOTE: the previous information was obtained from the February 2012 Oracle CPU.

EVRS

93/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.982

99.92nd percentile · FIRST

CISA DEADLINE

Mar 24, 2022

KEV since 2022 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.982 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Oracle has not commented on claims from a downstream vendor and third party researchers that this issue occurs because the AtomicReferenceArray class implementation does not ensure that the array is of the Object[] type, which allows attackers to cause a denial of service (JVM crash) or bypass Java sandbox restrictions. NOTE: this issue was originally mapped to CVE-2011-3571, but that identifier was already assigned to a different issue.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jre	1.5.0 1.6.0 1.7.0	no fixed version listed	NVD
debian linux	6.0 7.0	no fixed version listed	NVD
linux enterprise desktop	10	no fixed version listed	NVD
linux enterprise java	10 11	no fixed version listed	NVD
linux enterprise server	10 11	no fixed version listed	NVD
linux enterprise software development kit	11	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-43xj-964v-hcjf**NVD**nvd.nist.gov/vuln/detail/CVE-2012-0507**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD**euvd.enisa.europa.eu/vulnerability/EUVD-2012-0539**Current data** evulnable.com/vulnerability-management/cve/CVE-2012-0507

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.