

CVE-2010-0840

Oracle JRE Unspecified Vulnerability

Exigent

CISA KEV since May 25, 2022

Actively exploited

Public exploit module (Metasploit)

Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE and Java for Business 6 Update 18, 5.0 Update 23, and 1.4.2_25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

NOTE: the previous information was obtained from the March 2010 CPU. Oracle has not commented on claims from a reliable researcher that this is related to improper checks when executing privileged methods in the Java Runtime Environment (JRE), which allows attackers to

EVRS

86/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.963

99.88th percentile · FIRST

CISA DEADLINE

Jun 15, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.963 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

execute arbitrary code via (1) an untrusted object that extends the trusted class but has not modified a certain method, or (2) "a similar trust issue with interfaces," aka "Trusted Methods Chaining Remote Code Execution Vulnerability."

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jre	1.4.2_25 1.5.0 1.6.0	no fixed version listed	NVD
opensuse	11.0 11.1 11.2	no fixed version listed	NVD
ubuntu linux	8.04 8.10 9.04 9.10	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-8rrv-3xx7-wmfc	NVD	nvd.nist.gov/vuln/detail/CVE-2010-0840
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2010-0865
Current data	evulnable.com/vulnerability-management/cve/CVE-2010-0840		

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