

CVE-2013-2423

Oracle JRE Unspecified Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Public exploit module (Metasploit)

Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 7, allows remote attackers to affect integrity via unknown vectors related to HotSpot. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from the original researcher that this vulnerability allows remote attackers to bypass permission checks by the MethodHandles method and modify arbitrary public final fields using reflection and type confusion,

EVRS 75_{/100} Urgent priority	CVSS V3.1 3.7 Low · NVD	EPSS 0.852 99.72nd 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	0.852 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 3.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

as demonstrated using integer and double fields to disable the security manager.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jre	1.7.0	no fixed version listed	NVD
ubuntu linux	12.10	no fixed version listed	NVD
opensuse	12.3	no fixed version listed	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2013-2423

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2013-2369

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2013-2423

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