



# CVE-2026-22013

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

## Summary

<b>CVE</b>	CVE-2026-22013
<b>State</b>	PUBLISHED
<b>Assigner</b>	oracle
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 21:16:27 UTC
<b>Updated</b>	2026-04-22 21:24:26 UTC
<b>Description</b>	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from secalert\_us@oracle.com

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

**EPSS:** 0.000310000 probability, percentile 0.088810000 (date 2026-04-22)

**Problem Types:** CWE-693 | Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. | CWE-693 CWE-693 Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**None**

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 8u481	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 8u481-b50	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 8u481-perf	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 11.0.30	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 17.0.18	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 21.0.10	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 25.0.2	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle Java SE</a>	affected 26	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle GraalVM For JDK</a>	affected 17.0.18	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle GraalVM For JDK</a>	affected 21.0.10	Not specified
CNA	<a href="#">Oracle Corporation</a>	<a href="#">Oracle GraalVM Enterprise Edition</a>	affected 21.3.17	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.oracle.com/security-alerts/cpuapr2026.html">www.oracle.com/security-alerts/cpuapr2026.html</a>	<a href="mailto:secalert_us@oracle.com">secalert_us@oracle.com</a>	<a href="http://www.oracle.com">www.oracle.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)