



# CVE-2026-35255

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

## Summary

<b>CVE</b>	CVE-2026-35255
<b>State</b>	PUBLISHED
<b>Assigner</b>	oracle
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 10:16:19 UTC
<b>Updated</b>	2026-05-06 20:30:40 UTC
<b>Description</b>	Vulnerability in the Oracle Cloud Native Environment Command Line Interface product of Oracle Open Source Projects. The

## Risk And Classification

**Primary CVSS:** v3.1 6.6 MEDIUM from secalert\_us@oracle.com

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

**Problem Types:** CWE-94 | Vulnerability in the Oracle Cloud Native Environment Command Line Interface product of Oracle Open Source Projects. The supported versions that is affected is v2.3.2. Easily exploitable vulnerability allows unauthenticated attacker to compromise Oracle Cloud Native Environment Command Line Interface product via a malicious environment variable. Successful attacks of this vulnerability can result in Oracle Cloud Native Environment Command Line Interface allowing users to execute arbitrary code. | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	6.6	MEDIUM	<b>CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N</b>
3.1	CNA	DECLARED	6.6	MEDIUM	<b>CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N</b>

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Cloud Native Environment Command Line Interface	2.3.2	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Oracle Cloud Native Environment Command Line Interface	affected v2.3.2	Not specified

#### References

Reference	Source	Link	Tags
<a href="http://www.oracle.com/security-alerts/all-oracle-cves-outside-other-oracle-public-d...">www.oracle.com/security-alerts/all-oracle-cves-outside-other-oracle-public-d...</a>	secalert_us@oracle.com	<a href="http://www.oracle.com">www.oracle.com</a>	Not Applicable
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, ana

No vendor comments have been submitted for this CVE.

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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)