



# CVE-2026-35241

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-35241
<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 21:16:39 UTC
<b>Updated</b>	2026-04-22 21:24:26 UTC
<b>Description</b>	Vulnerability in the PeopleSoft Enterprise CS Student Records product of Oracle PeopleSoft (component: Research Trackir

## Risk And Classification

**Primary CVSS:** v3.1 5.7 MEDIUM from secalert\_us@oracle.com

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

**EPSS:** 0.000310000 probability, percentile 0.087960000 (date 2026-04-22)

**Problem Types:** CWE-284 | Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Records. 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 PeopleSoft Enterprise CS Student Records accessible data. | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert_us@oracle.com	Secondary	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	PeopleSoft Enterprise CS Student Records	affected 9.2 semver	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>	secalert_us@oracle.com	<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.

© 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/cve).

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)