CVE-2016-8285

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-8285
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-25 14:31:56 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Unspecified vulnerability in the PeopleSoft Enterprise HCM component in Oracle PeopleSoft Products 9.2 allows remote ad

Risk And Classification

Primary CVSS: v3.0 4.8 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:N

EPSS: 0.003440000 probability, percentile 0.570030000 (date 2026-05-09)

Problem Types: CWE-284 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:N
2.0	nvd@nist.gov	Primary	4.9		AV:N/AC:M/Au:S/C:P/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:M/Au:S/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Peoplesoft Enterprise Human Capital Management Candidate Gateway	9.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Oracle Critical Patch Update - October 2016
Oracle PeopleSoft Enterprise PeopleTools Multiple Flaws Let Remote Users Access and Modify Data on the Target System - SecurityTracker
Oracle PeopleSoft Enterprise HCM CVE-2016-8285 Remote Security Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**