



CVE-2017-10418

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

Summary

CVE	CVE-2017-10418
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-19 17:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: PeopleTools) allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via a crafted SOAP request, as demonstrated by the 'jws' endpoint. The vulnerability exists because the component does not properly validate the length of the request body. This vulnerability affects all versions of PeopleSoft Enterprise PT PeopleTools 8.56 and earlier.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All

References

Reference

- Oracle PeopleSoft Products Multiple Flaws Let Remote Users Access and Modify Data, Deny Service, and Gain Elevated Privileges on the T...
- Oracle PeopleSoft Enterprise PT PeopleTools CVE-2017-10418 Remote Security Vulnerability
- Oracle Critical Patch Update - October 2017
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#) 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

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