



CVE-2019-7442

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

Summary

CVE	CVE-2019-7442
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-08 21:29:00 UTC
Updated	2019-05-10 19:29:00 UTC
Description	An XML external entity (XXE) vulnerability in the Password Vault Web Access (PVWA) of CyberArk Enterprise Password V

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyberark	Enterprise Password Vault	All	All	All	All

References

Reference	Source	Link	Tag
CyberArk Enterprise Password Vault 10.7 XML External Entity Injection ~ Packet Storm	MISC	packetstormsecurity.com	
CyberArk Enterprise Password Vault – XML External Entity (XXE) Injection – Octopus Security	MISC	www.octurity.com	Exp
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)