



CVE-2018-9842

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-9842
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-12 15:29:00 UTC
Updated	2019-02-27 20:19:00 UTC
Description	CyberArk Password Vault before 9.7 allows remote attackers to obtain sensitive information from process memory by repla

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- CyberArk Password Vault Flaw Logon Response Lets Remote Users Obtain Potentially Sensitive Information from System Memory on the Tar
- SecurityFocus
- Full Disclosure: [RT-SA-2017-015] CyberArk Password Vault Memory Disclosure
- CyberArk < 10 - Memory Disclosure
- CyberArk 9.7 - Memory Disclosure - Windows remote Exploit
- RedTeam Pentesting GmbH - CyberArk Password Vault Memory Disclosure
- CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure - Linux dos Exploit
- 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.

© [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](#) 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](#)