CVE-2020-25738

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25738
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-27 06:15:00 UTC
Updated	2020-12-04 20:05:00 UTC
Description	CyberArk Endpoint Privilege Manager (EPM) 11.1.0.173 allows attackers to bypass a Credential Theft protection mechanis

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyberark	Endpoint Privilege Manager	11.1.0.173	All	All	All
Application	Cyberark	Endpoint Privilege Manager	11.1.0.173	All	All	All

References

Reference	Source	Link	Tags
Cyberark CVE-2020-25738 - Bypass Credential Theft Protection · GitHub	MISC	gist.github.com	Exploit, Third Party Advisory
Introducing CyberArk Endpoint Privilege Manager	MISC	www.cyberark.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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