



CVE-2020-28860

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

Summary

CVE	CVE-2020-28860
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-14 20:15:00 UTC
Updated	2020-12-15 16:41:00 UTC
Description	OpenAssetDigital Asset Management (DAM) through 12.0.19 does not correctly sanitize user supplied input, incorporating i

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openasset	Digital Asset Management	All	All	All	All

References

Reference	Source	L
OpenAsset Digital Asset Management SQL Injection ≈ Packet Storm	MISC	po
Full Disclosure: Authenticated blind SQL injection (SQLi) in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure	FULLDISC	se
OpenAsset Digital Asset Management Software	MISC	o
Advisory cve-2020-28860	MISC	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

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](#)