CVE-2017-20001

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-20001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-01 01:15:00 UTC
Updated	2021-01-12 15:34:00 UTC
Description	The AES encryption project 7.x and 8.x for Drupal does not sufficiently prevent attackers from decrypting data, aka SA-CON

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aes Encryption Project	Aes Encryption	All	All	All	All
Application	Aes Encryption Project	Aes Encryption	All	All	All	All

References

Reference	Source	Link	Tags
AES - Critical - Unsupported - SA-CONTRIB-2017-027 | Drupal.org	MISC	www.drupal.org	Third Party 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.

Free CVE JSON API cve.report/api

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