CVE-2015-7764

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

Summary

CVE	CVE-2015-7764
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-09 16:29:00 UTC
Updated	2019-12-11 21:22:00 UTC
Description	Lemur 0.1.4 does not use sufficient entropy in its IV when encrypting AES in CBC mode.

Risk And Classification

Problem Types: CWE-331

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netflix	Lemur	0.1.4	All	All	All
Application	Netflix	Lemur	0.1.4	All	All	All

References

Reference	Source	Link	Tags
Certificates encrypted with static IV per key · Issue #117 · Netflix/lemur · GitHub	CONFIRM	github.com	Third Party Advisc
oss-security - Re: CVE request for sqlalchemy-utils	MLIST	www.openwall.com	Mailing List, Third
EncryptedType uses static IV per key · Issue #166 · kvesteri/sqlalchemy-utils · GitHub	CONFIRM	github.com	Third Party Advisc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

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 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.

Free CVE JSON API cve.report/api

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