



CVE-2018-6829

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

Summary

CVE	CVE-2018-6829
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-07 23:29:00 UTC
Updated	2020-01-15 20:15:00 UTC
Description	cipher/algamal.c in Libgrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnupg	Libgrypt	All	All	All	All

References

Reference	Source	Link	Tags
Home · weikengchen/attack-on-libgrypt-ElGamal Wiki · GitHub	MISC	github.com	Expl
Attack on libgrypt's ElGamal Encryption with Proof of Concept (PoC)	MISC	lists.gnupg.org	Issue
GitHub - weikengchen/attack-on-libgrypt-ElGamal: Attack on the ElGamal Implementation of libgrypt	MISC	github.com	Third
Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)