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/elgamal.c in Libgcrypt 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	Libgcrypt	All	All	All	All

References

Reference	Source	Link	Tags
Home · weikengchen/attack-on-libgcrypt-elgamal Wiki · GitHub	MISC	github.com	Explo
Attack on libgcrypt's ElGamal Encryption with Proof of Concept (PoC)	MISC	lists.gnupg.org	Issue
GitHub - weikengchen/attack-on-libgcrypt-elgamal: Attack on the ElGamal Implementation of libgcrypt	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.

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