CVE-2019-12904

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-12904
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-20 00:15:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	** DISPUTED ** In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack bec

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnupg	Libgcrypt	1.8.4	All	All	All
Application	Gnupg	Libgcrypt	1.8.4	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache.org
GCM: move look-up table to .data section and unshare between processes · gpg/libgcrypt@a4c561a · GitHub	MISC	github.com
[security-announce] openSUSE-SU-2019:1792-1: moderate: Security update f	SUSE	lists.opensuse.c
AES: move look-up tables to .data section and unshare between processes · gpg/libgcrypt@daedbbb · GitHub	MISC	github.com
[mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar		lists.apache.org
⚓ T4541 C implementation of AES is vulnerable to side-channel attacks	MISC	dev.gnupg.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500293 Alpine Linux Security Update for libgcrypt

504059 Alpine Linux Security Update for libgcrypt

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)