CVE-2017-0379

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-0379
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-29 22:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	Libgcrypt before 1.8.1 does not properly consider Curve25519 side-channel attacks, which makes it easier for attackers to c

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All

References

Reference
git.gnupg.org Git - libgcrypt.git/commit
#873383 - libgcrypt20: CVE-2017-0379: side-channel attack on Curve25519 - Debian Bug report logs
libgcrypt CVE-2017-0379 Information Disclosure Vulnerability
CPU July 2018
MySQL Multiple Flaws Let Remote Users Access and Gain Elevated Privileges, Remote Authenticated and Local Users Deny Service, and Re
July 2018 MySQL Vulnerabilities in NetApp Products | NetApp Product Security
CVE-2017-0379
Oracle Critical Patch Update - January 2019
Cryptology ePrint Archive: Report 2017/806
[SECURITY] [DSA 3959-1] libgcrypt20 security update
Debian -- Security Information -- DSA-3959-1 libgcrypt20

git.gnupg.org Git - libgcrypt.git/commit
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.