



# CVE-2017-0379

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

## Summary

<b>CVE</b>	CVE-2017-0379
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-29 22:29:00 UTC
<b>Updated</b>	2023-11-07 02:37:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Libgcrypt</a>	All	All	All	All

## References

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

git.gnupg.org Git - libgcrpt.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.

© [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 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](#)**