



CVE-2017-7526

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

Summary

CVE	CVE-2017-7526
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 13:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	libcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 whil

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnupg	Libcrypt	All	All	All	All
Application	Gnupg	Libcrypt	All	All	All	All

References

Reference
Cryptology ePrint Archive: Report 2017/627
git.gnupg.org Git - libcrypt.git/commit

git.gnupg.org Git - libgcrpt.git/commit

Debian -- Security Information -- DSA-3901-1 libgcrpt20

git.gnupg.org Git - libgcrpt.git/commit

USN-3733-1: GnuPG vulnerability | Ubuntu security notices

git.gnupg.org Git - libgcrpt.git/commit

USN-3733-2: GnuPG vulnerability | Ubuntu security notices

git.gnupg.org Git - libgcrpt.git/commit

1466265 – (CVE-2017-7526) CVE-2017-7526 libgcrpt: Use of left-to-right sliding window method allows full RSA key recovery

git.gnupg.org Git - libgcrpt.git/commit

[Announce] Libgcrpt 1.7.8 released to fix CVE-2017-7526

Libgcrpt CVE-2017-7526 Information Disclosure Vulnerability

Debian -- Security Information -- DSA-3960-1 gnupg

Libgcrpt RSA-1024 Sliding-Window Expansion Side Channel Attack Lets Remote Users Recover Keys Used by the Target System in Certain

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500359](#) Alpine Linux Security Update for gnupg1

[671105](#) EulerOS Security Update for libgcrpt (EulerOS-SA-2019-2205)

© [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](#)