



CVE-2017-9526

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

Summary

CVE	CVE-2017-9526
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-11 02:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	In Libcrypt before 1.7.7, an attacker who learns the EdDSA session key (from side-channel observation during the signing

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnupg	Libcrypt	All	All	All	All

References

Reference	Source	Link	Tags
git.gnupg.org Git - libcrypt.git/commit		git.gnupg.org	
CPU July 2018	CONFIRM	www.oracle.com	
git.gnupg.org Git - libcrypt.git/commit	CONFIRM	git.gnupg.org	Issue Tracking
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com	
Debian -- Security Information -- DSA-3880-1 libcrypt20	DEBIAN	www.debian.org	
Libcrypt 'cipher/ecc-eddsa.c' Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party A
git.gnupg.org Git - libcrypt.git/commit		git.gnupg.org	
Bug 1042326 – VUL-0: CVE-2017-9526: libcrypt: timing attack on EdDSA session key	CONFIRM	bugzilla.suse.com	Issue Tracking
git.gnupg.org Git - libcrypt.git/commit	CONFIRM	git.gnupg.org	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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](#)