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 Libgcrypt 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	Libgcrypt	All	All	All	All

References

Reference	Source	Link	Tags
git.gnupg.org Git - libgcrypt.git/commit		git.gnupg.org	
CPU July 2018	CONFIRM	www.oracle.com	
git.gnupg.org Git - libgcrypt.git/commit	CONFIRM	git.gnupg.org	Issue Tracki
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com	
Debian -- Security Information -- DSA-3880-1 libgcrypt20	DEBIAN	www.debian.org	
Libgcrypt 'cipher/ecc-eddsa.c' Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party A
git.gnupg.org Git - libgcrypt.git/commit		git.gnupg.org	
Bug 1042326 – VUL-0: CVE-2017-9526: libgcrypt: timing attack on EdDSA session key	CONFIRM	bugzilla.suse.com	Issue Tracki
git.gnupg.org Git - libgcrypt.git/commit	CONFIRM	git.gnupg.org	Issue Tracki
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report