CVE-2019-13627

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-13627
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-25 15:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1

Risk And Classification

Problem Types: CWE-203

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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	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	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	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	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.6.3-2+deb8u4	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.6.3-2\+deb8u4	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.7.6-2+deb9u3	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.7.6-2\+deb9u3	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.8.4-5	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.6.3-2\+deb8u4	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.7.6-2\+deb9u3	All	All	All
Application	Libgcrypt20 Project	Libgcrypt20	1.8.4-5	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link	Tags
USN-4236-2: Libgcrypt vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Adviso
USN-4236-1: Libgcrypt vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Adviso
[SECURITY] [DLA 1931-2] libgcrypt20 regression update	MLIST	lists.debian.org	Third Party Adviso
Release libgcrypt-1.8.5 · gpg/libgcrypt · GitHub	MISC	github.com	Third Party Adviso
[security-announce] openSUSE-SU-2019:2161-1: moderate: Security update f	SUSE	lists.opensuse.org	Third Party Adviso
[security-announce] openSUSE-SU-2020:0022-1: moderate: Security update f	SUSE	lists.opensuse.org	Third Party Adviso
minerva.crocs.fi.muni.cz	MISC	minerva.crocs.fi.muni.cz	Third Party Adviso
CVE-2019-13627	MISC	security-tracker.debian.org	Third Party Adviso
Libgcrypt: Side-channel attack (GLSA 202003-32) — Gentoo security	GENTOO	security.gentoo.org	Third Party Adviso
[SECURITY] [DLA 1931-1] libgcrypt20 security update	MLIST	lists.debian.org	Mailing List, Third
oss-security - Minerva: ECDSA key recovery from bit-length leakage	MLIST	www.openwall.com	Mailing List, Third
USN-4236-3: Libgcrypt vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296079 Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

500294 Alpine Linux Security Update for libgcrypt

504060 Alpine Linux Security Update for libgcrypt

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

770068 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

940271 AlmaLinux Security Update for libgcrypt (ALSA-2020:4482)

960748 Rocky Linux Security Update for libgcrypt (RLSA-2020:4482)

© 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 registred 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