



# CVE-2018-0495

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

## Summary

<b>CVE</b>	CVE-2018-0495
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-13 23:29:00 UTC
<b>Updated</b>	2023-11-07 02:51:00 UTC
<b>Description</b>	Libcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can k

## 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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	Libgcrypt	All	All	All	All
Application	Oracle	Traffic Director	11.1.1.9.0	All	All	All
Application	Oracle	Traffic Director	11.1.1.9.0	All	All	All
Application	Redhat	Ansible Tower	3.3	All	All	All
Application	Redhat	Ansible Tower	3.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

## References

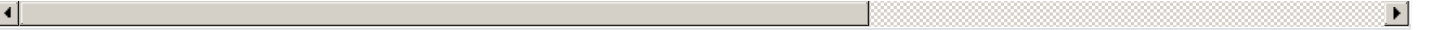
Reference	S
Red Hat Customer Portal	R
⌘ T4011 CVE-2018-0495	M
Red Hat Customer Portal	R
[Announce] Libgcrypt 1.8.3 and 1.7.10 to fix CVE-2018-0495	M
git.gnupg.org Git - libgcrypt.git/commit	
Red Hat Customer Portal	R
[SECURITY] [DLA 1405-1] libgcrypt20 security update	M
Debian -- Security Information -- DSA-4231-1 libgcrypt20	D
Libgcrypt ECDSA Signature Calculation Timing Flaw Lets Local Users Obtain Private DSA Keys on the Target System - SecurityTracker	S
USN-3689-1: Libgcrypt vulnerability   Ubuntu security notices	U
Red Hat Customer Portal	R
USN-3850-1: NSS vulnerabilities   Ubuntu security notices	U
www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-numbe...	M
Red Hat Customer Portal	R
git.gnupg.org Git - libgcrypt.git/commit	M
USN-3850-2: NSS vulnerabilities   Ubuntu security notices	U
OpenBSD ECDSA Signature Calculation Timing Flaw Lets Local Users Obtain Private DSA Keys on the Target System - SecurityTracker	S
USN-3689-2: Libgcrypt vulnerability   Ubuntu security notices	U
USN-3692-1: OpenSSL vulnerabilities   Ubuntu security notices	U
Red Hat Customer Portal	R
USN-3692-2: OpenSSL vulnerabilities   Ubuntu security notices	U

CVE Program record

C

NVD vulnerability detail

N



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[296092](#) Oracle Solaris 11.4 Support Repository Update (SRU) 7.1.4 Missing (CPUJAN2019)

[377300](#) Alibaba Cloud Linux Security Update for nss, nss-softokn, nss-util, and nspr (ALINUX2-SA-2019:0104)

[500292](#) Alpine Linux Security Update for libgcrypt

[500368](#) Alpine Linux Security Update for libressl

[504058](#) Alpine Linux Security Update for libgcrypt

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

[690634](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libgcrypt (9b5162de-6f39-11e8-818e-e8e0b747a45a)

© [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](#)**