

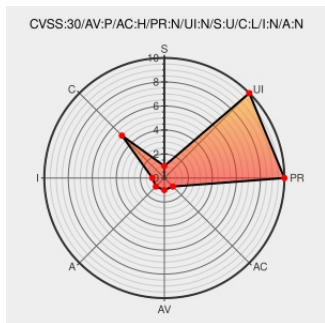


CVE-2015-7511

Published on: 04/19/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

CVE-2015-7511

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Libcrypt before 1.6.5 does not properly perform elliptic-point curve multiplication during decryption, which makes it easier for physically proximate attackers to extract ECDH keys by measuring electromagnetic emanations.

CVE-2015-7511 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **2 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[Announce] Libcrypt 1.6.5 with security fix released	Vendor Advisory lists.gnupg.org text/html	MLIST [gnupg-announce] 20160209 [Announce] Libcrypt 1.6.5 with security fix released
[SECURITY] Fedora 24 Update: libcrypt-1.6.5-1.fc24 -	lists.fedoraproject.org	FEDORA FEDORA-2016-83cd045bcc

package-announce - Fedora Mailing-Lists	text/html	
GNU Libcrypt CVE-2015-7511 Security Bypass Vulnerability	cve.report (archive) text/html	 BID 83253
Debian -- Security Information -- DSA-3478-1 libgcrpt11	www.debian.org Depreciated Link text/html	 DEBIAN DSA-3478
openSUSE-SU-2016:1227-1: moderate: Security update for libgcrpt	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1227
Debian -- Security Information -- DSA-3474-1 libgcrpt20	www.debian.org Depreciated Link text/html	 DEBIAN DSA-3474
ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs	www.cs.tau.ac.il text/html	 MISC www.cs.tau.ac.il/~tromer/ecdh/
libgcrpt: Multiple vulnerabilities (GLSA 201610-04) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201610-04
USN-2896-1: Libgcrpt vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2896-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	15.10	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	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

System						
Application	Gnupg	Libgcrypt	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:***:***:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:***:***:***:						
cpe:2.3:o:debian:debian_linux:7.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:8.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:7.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:8.0:***:***:***:						
cpe:2.3:a:gnupg:libgcrypt:***:***:***:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID →		