



# CVE-2014-5270

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

## Summary

<b>CVE</b>	CVE-2014-5270
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-10-10 01:55:00 UTC
<b>Updated</b>	2017-11-04 01:29:00 UTC
<b>Description</b>	Libgcrypt before 1.5.4, as used in GnuPG and other products, does not properly perform ciphertext normalization and ciphe

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Gnupg	Libgcrypt	1.4.0	All	All	All
Application	Gnupg	Libgcrypt	1.4.3	All	All	All
Application	Gnupg	Libgcrypt	1.4.4	All	All	All
Application	Gnupg	Libgcrypt	1.4.5	All	All	All
Application	Gnupg	Libgcrypt	1.4.6	All	All	All
Application	Gnupg	Libgcrypt	1.5.0	All	All	All
Application	Gnupg	Libgcrypt	1.5.1	All	All	All
Application	Gnupg	Libgcrypt	1.5.2	All	All	All
Application	Gnupg	Libgcrypt	1.4.0	All	All	All
Application	Gnupg	Libgcrypt	1.4.3	All	All	All
Application	Gnupg	Libgcrypt	1.4.4	All	All	All
Application	Gnupg	Libgcrypt	1.4.5	All	All	All
Application	Gnupg	Libgcrypt	1.4.6	All	All	All
Application	Gnupg	Libgcrypt	1.5.0	All	All	All
Application	Gnupg	Libgcrypt	1.5.1	All	All	All

Application	<a href="#">Gnupg</a>	<a href="#">Libgcrypt</a>	1.5.2	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Libgcrypt</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - Re: CVE request: libgcrypt, ELGAMAL side-channel attack	MLIST	<a href="https://openwall.com">openwall.com</a>	Mailing List, Third Party Advisory
Debian -- Security Information -- DSA-3073-1 libgcrypt11	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
<a href="http://www.cs.tau.ac.il/~tromer/handsoff">www.cs.tau.ac.il/~tromer/handsoff</a>	MISC	<a href="http://www.cs.tau.ac.il">www.cs.tau.ac.il</a>	Technical Description
[Announce] [security fix] Libgcrypt and GnuPG	MLIST	<a href="https://lists.gnupg.org">lists.gnupg.org</a>	Patch, Vendor Advisory
Debian -- Security Information -- DSA-3024-1 gnupg	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[671105](#) EulerOS Security Update for libgcrypt (EulerOS-SA-2019-2205)

© [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](https://status.cve.report)