CVE-2014-5270

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-5270
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-10 01:55:00 UTC
Updated	2017-11-04 01:29:00 UTC
Description	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	Gnupg	Libgcrypt	1.5.2	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: CVE request: libgcrypt, ELGAMAL side-channel attack	MLIST	openwall.com	Mailing List, Third Party Advisory
Debian -- Security Information -- DSA-3073-1 libgcrypt11	DEBIAN	www.debian.org	Third Party Advisory
www.cs.tau.ac.il/~tromer/handsoff	MISC	www.cs.tau.ac.il	Technical Description
[Announce] [security fix] Libgcrypt and GnuPG	MLIST	lists.gnupg.org	Patch, Vendor Advisory
Debian -- Security Information -- DSA-3024-1 gnupg	DEBIAN	www.debian.org	
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

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