CVE-2014-3591

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-3591
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-29 22:15:00 UTC
Updated	2019-12-05 18:06:00 UTC
Description	Libgcrypt before 1.6.3 and GnuPG before 1.4.19 does not implement ciphertext blinding for Elgamal decryption, which allow

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	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
Application	Gnupg	Gnupg	All	All	All	All
Application	Gnupg	Gnupg	All	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All

References

Reference	Source	Link	Tags
[Announce] Libgcrypt 1.6.3 released (with SCA fix)	MISC	lists.gnupg.org	Patch, Ven
Stealing Keys from PCs by Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation	MISC	www.cs.tau.ac.il	Third Party
Debian -- Security Information -- DSA-3185-1 libgcrypt11	MISC	www.debian.org	Third Party
[Announce] GnuPG 1.4.19 released (with SCA fix)	MISC	lists.gnupg.org	Patch, Rele
Debian -- Security Information -- DSA-3184-1 gnupg	MISC	www.debian.org	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296059 Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)