CVE-2015-0837

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-0837
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-29 22:15:00 UTC
Updated	2019-12-14 13:59:00 UTC
Description	The mpi_powm function in Libgcrypt before 1.6.3 and GnuPG before 1.4.19 allows attackers to obtain sensitive information

Risk And Classification

Problem Types: CWE-203

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
Debian -- Security Information -- DSA-3185-1 libgcrypt11	MISC	www.debian.org	Third Party Advisory
[Announce] GnuPG 1.4.19 released (with SCA fix)	CONFIRM	lists.gnupg.org	Mailing List, Vendor
Last-Level Cache Side-Channel Attacks are Practical - IEEE Conference Publication	MISC	ieeexplore.ieee.org	Third Party Advisory
Debian -- Security Information -- DSA-3184-1 gnupg	MISC	www.debian.org	Third Party Advisory
[Announce] Libgcrypt 1.6.3 released (with SCA fix)	CONFIRM	lists.gnupg.org	Mailing List, Vendor
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.

There are currently no legacy QID mappings associated with this CVE.