



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	Libcrypt 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	Libcrypt	All	All	All	All
Application	Gnupg	Libcrypt	All	All	All	All

References

Reference	Source	Link	Tags
[Announce] Libcrypt 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 libcrypt11	MISC	www.debian.org	Third Party
[Announce] GnuPG 1.4.19 released (with SCA fix)	MISC	lists.gnupg.org	Patch, Relk
Debian -- Security Information -- DSA-3184-1 gnupg	MISC	www.debian.org	Third Party
CVE Program record	CVE.ORG	www.cve.org	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)

© [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](#)