CVE-2021-40528

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-40528
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-06 19:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	The ElGamal implementation in Libgcrypt before 1.9.4 allows plaintext recovery because, during interaction between two cr

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnupg	Libgcrypt	All	All	All	All

References

Reference	Source	Link	Tags
Cryptology ePrint Archive: Report 2021/923 - On the (in)security of ElGamal in OpenPGP	MISC	eprint.iacr.org	
libgcrypt: Multiple Vulnerabilities (GLSA 202210-13) — Gentoo security	GENTOO	security.gentoo.org	
git.gnupg.org Git - libgcrypt.git/commit		git.gnupg.org	
On the (in)security of ElGamal in OpenPGP - Part II - Syssec@IBM Research	MISC	ibm.github.io	
On the (in)security of ElGamal in OpenPGP - Part I - Syssec@IBM Research	MISC	ibm.github.io	
git.gnupg.org Git - libgcrypt.git/commit	MISC	git.gnupg.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159956 Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2022-5311)

159970 Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2022-9564)

180558 Debian Security Update for libgcrypt20 (CVE-2021-40528)

198503 Ubuntu Security Notification for Libgcrypt Vulnerabilities (USN-5080-1)

240533 Red Hat Update for libgcrypt (RHSA-2022:5311)

296065 Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)

377331 Alibaba Cloud Linux Security Update for libgcrypt (ALINUX3-SA-2022:0129)

500296 Alpine Linux Security Update for libgcrypt

671173 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2914)

671179 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2922)

671236 EulerOS Security Update for libgcrypt (EulerOS-SA-2022-1173)

671279 EulerOS Security Update for libgcrypt (EulerOS-SA-2022-1228)

671326 EulerOS Security Update for libgcrypt (EulerOS-SA-2022-1209)

710653 Gentoo Linux libgcrypt Multiple Vulnerabilities (GLSA 202210-13)

900444 Common Base Linux Mariner (CBL-Mariner) Security Update for libgcrypt (5450)

940597 AlmaLinux Security Update for libgcrypt (ALSA-2022:5311)

960401 Rocky Linux Security Update for libgcrypt (RLSA-2022:5311)