



# CVE-2021-40528

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-40528
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-09-06 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:38:00 UTC
<b>Description</b>	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	<a href="#">Gnupg</a>	<a href="#">Libgcrypt</a>	All	All	All	All

## References

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

© [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](#)**