CVE-2021-33560

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-33560
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-08 11:15:00 UTC
Updated	2023-11-07 03:35:00 UTC
Description	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Debian	Debian Linux	9.0	All
Operating System	Fedoraproject	Fedora	33	All
Operating System	Fedoraproject	Fedora	34	All
Application	Gnupg	Libgcrypt	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	1.11.0	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.9.0	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	1.14.0	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	1.15.0	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	1.15.1	All
Application	Oracle	Communications Cloud Native Core Network Slice Selection Function	1.8.0	All
Application	Oracle	Communications Cloud Native Core Service Communication Proxy	1.15.0	All

References

Reference	Source	Link	Tag
libgcrypt: Multiple Vulnerabilities (GLSA 202210-13) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 34 Update: libgcrypt-1.9.3-3.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
⚓ T5466 Release Libgcrypt 1.8.8	MISC	dev.gnupg.org	
[SECURITY] [DLA 2691-1] libgcrypt20 security update	MLIST	lists.debian.org	
[SECURITY] Fedora 33 Update: libgcrypt-1.8.8-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
⚓ T5305 Release Libgcrypt 1.9.3	MISC	dev.gnupg.org	
[SECURITY] Fedora 33 Update: libgcrypt-1.8.8-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
rCe8b7f10be275	MISC	dev.gnupg.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
[SECURITY] Fedora 34 Update: libgcrypt-1.9.3-3.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
⚓ T5328 On the (in)security of Elgamal in OpenPGP	MISC	dev.gnupg.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159510 Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2021-4409)
- 159742 Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2022-9263)
- 178682 Debian Security Update for libgcrypt20 (DLA 2691-1)
- 183602 Debian Security Update for libgcrypt20 (CVE-2021-33560)
- 198503 Ubuntu Security Notification for Libgcrypt Vulnerabilities (USN-5080-1)
- 239828 Red Hat Update for libgcrypt (RHSA-2021:4409)
- 281670 Fedora Security Update for libgcrypt (FEDORA-2021-24d4e06195)
- 281672 Fedora Security Update for libgcrypt (FEDORA-2021-31fdc84207)
- 296059 Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)
- 296060 Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021)
- 353205 Amazon Linux Security Advisory for libgcrypt : ALAS-2022-1578
- 353209 Amazon Linux Security Advisory for libgcrypt : ALAS2-2022-1769
- 354634 Amazon Linux Security Advisory for libgcrypt : AL2012-2022-366
- 500295 Alpine Linux Security Update for libgcrypt

501746 Alpine Linux Security Update for libgcrypt

504061 Alpine Linux Security Update for libgcrypt

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

670637 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2395)

670711 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2469)

670745 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2503)

670774 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2532)

670798 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2556)

670963 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2590)

671182 EulerOS Security Update for libgcrypt (EulerOS-SA-2021-2935)

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

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

750708 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2155-1)

750709 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2157-1)

750711 SUSE Enterprise Linux Security Update for libgcrypt (SUSE-SU-2021:2156-1)

750728 OpenSUSE Security Update for libgcrypt (openSUSE-SU-2021:0919-1)

750778 OpenSUSE Security Update for libgcrypt (openSUSE-SU-2021:2157-1)

900144 CBL-Mariner Linux Security Update for libgcrypt 1.8.7

903176 Common Base Linux Mariner (CBL-Mariner) Security Update for libgcrypt (4347)

940222 AlmaLinux Security Update for libgcrypt (ALSA-2021:4409)

960079 Rocky Linux Security Update for libgcrypt (RLSA-2021:4409)