



CVE-2020-36242

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-36242
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-07 20:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	In the cryptography package before 3.3.2 for Python, certain sequences of update calls to symmetrically encrypt multi-GB v

Risk And Classification

Problem Types: CWE-787 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	U
Application	Cryptography Project	Cryptography	All	AI
Application	Cryptography Project	Cryptography	All	AI
Operating System	Fedoraproject	Fedora	33	AI
Operating System	Fedoraproject	Fedora	33	AI
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	AI

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: python-cryptography-3.2.1-2.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com
Comparing 3.3.1...3.3.2 · pyca/cryptography · GitHub	CONFIRM	github.com
[SECURITY] Fedora 33 Update: python-cryptography-3.2.1-2.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
Fernet fails to encrypt/decrypt large data · Issue #5615 · pyca/cryptography · GitHub	MISC	github.com
cryptography/CHANGELOG.rst at main · pyca/cryptography · GitHub	CONFIRM	github.com
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159194	Oracle Enterprise Linux Security Update for python-cryptography (ELSA-2021-1608)
239330	Red Hat Update for python-cryptography (RHSA-2021:1608)
239580	Red Hat Update for rh-python38 (RHSA-2021:3254)
296067	Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)
377334	Alibaba Cloud Linux Security Update for python-cryptography (ALINUX3-SA-2022:0083)
501475	Alpine Linux Security Update for py3-cryptography
502338	Alpine Linux Security Update for py3-cryptography
670494	EulerOS Security Update for python-cryptography (EulerOS-SA-2021-2252)
670520	EulerOS Security Update for python-cryptography (EulerOS-SA-2021-2278)
750342	OpenSUSE Security Update for python-cryptography (openSUSE-SU-2021:0349-1)
753738	SUSE Enterprise Linux Security Update for python-cryptography, python-cryptography-vectors (SUSE-SU-2023:0604-1)
754157	SUSE Enterprise Linux Security Update for grpc, protobuf, python-Deprecated, python-PyGithub, python-aioccontextvars, python-avro, python-bcrypt, python-cryptography, python-cryptography-vectors, python-google-api-core, pyt (SUSE-SU-2023:2783-1)
754878	SUSE Enterprise Linux Security Update for grpc, protobuf, python-DEPRECATED, python-PyGithub, python-aioccontextvars, python-avro, python-bcrypt, python-cryptography, python-cryptography-vectors, python-google-api-core, pyt (SUSE-SU-2023:2783-2)
900039	CBL-Mariner Linux Security Update for python-cryptography 2.3.1
903166	Common Base Linux Mariner (CBL-Mariner) Security Update for python-cryptography (3875)
940282	AlmaLinux Security Update for python-cryptography (ALSA-2021:1608)
960766	Rocky Linux Security Update for python-cryptography (RLSA-2021:1608)
981929	Python (pip) Security Update for cryptography (GHSA-rhm9-p9w5-fwm7)

© 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](#)