



CVE-2020-25659

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

Summary

CVE	CVE-2020-25659
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-11 16:15:00 UTC
Updated	2023-02-09 02:25:00 UTC
Description	python-cryptography 3.2 is vulnerable to Bleichenbacher timing attacks in the RSA decryption API, via timed processing of

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All
Application	Python-cryptography Project	Python-cryptography	3.2	All
Application	Python-cryptography Project	Python-cryptography	3.2	All

References

Reference	Source	Link
Attempt to mitigate Bleichenbacher attacks on RSA decryption by alex · Pull Request #5507 · pyca/cryptography · GitHub	MISC	github
Oracle Critical Patch Update Advisory - April 2022	MISC	www
Oracle Critical Patch Update Advisory - July 2022	N/A	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

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)
296069 Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)
377334 Alibaba Cloud Linux Security Update for python-cryptography (ALINUX3-SA-2022:0083)
501474 Alpine Linux Security Update for py3-cryptography
674135 EulerOS Security Update for python-cryptography (EulerOS-SA-2024-1494)
674139 EulerOS Security Update for python-cryptography (EulerOS-SA-2024-1515)
750515 OpenSUSE Security Update for python-cryptography (openSUSE-SU-2020:2173-1)
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)
900225 CBL-Mariner Linux Security Update for python-cryptography 2.3.1
903449 Common Base Linux Mariner (CBL-Mariner) Security Update for python-cryptography (3734)
940282 AlmaLinux Security Update for python-cryptography (ALSA-2021:1608)
960766 Rocky Linux Security Update for python-cryptography (RLSA-2021:1608)
983257 Python (pip) Security Update for cryptography (GHSA-hggm-jpg3-v476)

© [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](#)