



CVE-2023-38325

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-38325
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-14 20:15:00 UTC
Updated	2023-11-07 04:17:00 UTC
Description	The cryptography package before 41.0.2 for Python mishandles SSH certificates that have critical options.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptography Project	Cryptography	All	All	All	All

References

Reference	Source	Link
CVE-2023-38325 Python Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 38 Update: python-yfinance-0.2.28-4.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Comparing 41.0.1...41.0.2 · pyca/cryptography · GitHub	MISC	github.com
cryptography · PyPI	MISC	pypi.org
SSH certificate encoding/parsing incompatibility with OpenSSH · Issue #9207 · pyca/cryptography · GitHub	MISC	github.com
Fix encoding of SSH certs with critical options by lkubb · Pull Request #9208 · pyca/cryptography · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: python-yfinance-0.2.28-4.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
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

[284434](#) Fedora Security Update for python (FEDORA-2023-2b0f2e4bc3)

[285299](#) Fedora Security Update for python (FEDORA-2023-31d5d51a2d)

[506173](#) Alpine Linux Security Update for py3-cryptography

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)