



CVE-2022-48565

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

Summary

CVE	CVE-2022-48565
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-22 19:16:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	An XML External Entity (XXE) issue was discovered in Python through 3.9.1. The plistlib module no longer accepts entity de

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Python	Python	All	All	All	All
Application	Python	Python	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: python2.7-2.7.18-35.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: python2.7-2.7.18-35.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: python2.7-2.7.18-35.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 38 Update: python2.7-2.7.18-35.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 3614-1] python3.7 security update	MLIST	lists.debian.org
[SECURITY] Fedora 39 Update: python2.7-2.7.18-35.fc39 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 3575-1] python2.7 security update	MLIST	lists.debian.org
[SECURITY] Fedora 39 Update: python2.7-2.7.18-35.fc39 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Issue 42051: [security] Avoid plistlib XML vulnerabilities by rejecting entity directives - Python tracker	MISC	bugs.python.org
CVE-2022-48565 Python Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

284647 Fedora Security Update for python2.7 (FEDORA-2023-e47078af3e)
284648 Fedora Security Update for python2.7 (FEDORA-2023-348a0dbcf3)
285201 Fedora Security Update for python2.7 (FEDORA-2023-ea38857cc3)
356421 Amazon Linux Security Advisory for python3 : ALAS2-2023-2317
356554 Amazon Linux Security Advisory for python27 : ALAS-2023-1880
356576 Amazon Linux Security Advisory for python : ALAS2-2023-2330
378864 Python Extensible Markup Language (XML) External Entity Vulnerability
6000148 Debian Security Update for python2.7 (DLA 3575-1)
6000279 Debian Security Update for python3.7 (DLA 3614-1)
673325 EulerOS Security Update for python2 (EulerOS-SA-2024-1290)
673594 EulerOS Security Update for python (EulerOS-SA-2024-1160)
673778 EulerOS Security Update for python3 (EulerOS-SA-2024-1291)
755046 SUSE Enterprise Linux Security Update for python (SUSE-SU-2023:4001-1)
755169 SUSE Enterprise Linux Security Update for python (SUSE-SU-2023:4220-1)

© [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](#)