



CVE-2020-5312

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

Summary

CVE	CVE-2020-5312
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-03 01:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Python	Pillow	All	All	All	All

Application	Python	Pillow	All	All	All	All
References						
Reference				Source	Link	
[SECURITY] Fedora 31 Update: python-pillow-6.2.2-1.fc31 - package-announce - Fedora Mailing-Lists				FEDORA	lists.fedoraproject.org	
6.2.2 — Pillow (PIL Fork) 7.0.0 documentation				MISC	pillow.readthedocs.io	
Red Hat Customer Portal				REDHAT	access.redhat.com	
Red Hat Customer Portal				REDHAT	access.redhat.com	
[SECURITY] Fedora 31 Update: python-pillow-6.2.2-1.fc31 - package-announce - Fedora Mailing-Lists					lists.fedoraproject.org	
Red Hat Customer Portal				REDHAT	access.redhat.com	
Red Hat Customer Portal				REDHAT	access.redhat.com	
Catch PCX P mode buffer overrun · python-pillow/Pillow@93b22b8 · GitHub				MISC	github.com	
Red Hat Customer Portal				REDHAT	access.redhat.com	
Red Hat Customer Portal				REDHAT	access.redhat.com	
[SECURITY] Fedora 30 Update: python-pillow-5.4.1-4.fc30 - package-announce - Fedora Mailing-Lists				FEDORA	lists.fedoraproject.org	
Debian -- Security Information -- DSA-4631-1 pillow				DEBIAN	www.debian.org	
USN-4272-1: Pillow vulnerabilities Ubuntu security notices Ubuntu				UBUNTU	usn.ubuntu.com	
[SECURITY] Fedora 30 Update: python-pillow-5.4.1-4.fc30 - package-announce - Fedora Mailing-Lists					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

- [296076](#) Oracle Solaris 11.4 Support Repository Update (SRU) 19.3.0 Missing (CPUJAN2020)
- [377249](#) Alibaba Cloud Linux Security Update for python-pillow (ALINUX2-SA-2020:0024)
- [500780](#) Alpine Linux Security Update for py3-pillow
- [505314](#) Alpine Linux Security Update for py3-pillow
- [980225](#) Python (pip) Security Update for Pillow (GHSA-p49h-hjvm-jg3h)

© 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