



CVE-2021-34552

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-34552 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-07-13 17:15:00 UTC |
| Updated | 2023-11-07 03:36:00 UTC |
| Description | Pillow through 8.2.0 and PIL (aka Python Imaging Library) through 1.1.7 allow an attacker to pass controlled parameters dir |

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|--------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Application | Python | Pillow | All | All | All | All |
| Application | Python | Pillow | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|-----------------------------------|
| [SECURITY] Fedora 33 Update: mingw-python-pillow-7.2.0-7.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproje |
| Release Notes — Pillow (PIL Fork) 8.2.0 documentation | MISC | pillow.readthedc |
| [SECURITY] Fedora 34 Update: mingw-python-pillow-8.1.2-3.fc34 - package-announce - Fedora Mailing-Lists | | lists.fedoraproje |
| [SECURITY] Fedora 33 Update: mingw-python-pillow-7.2.0-7.fc33 - package-announce - Fedora Mailing-Lists | | lists.fedoraproje |
| Pillow: Multiple Vulnerabilities (GLSA 202211-10) — Gentoo security | GENTOO | security.gentoo. |
| [SECURITY] Fedora 34 Update: mingw-python-pillow-8.1.2-3.fc34 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproje |
| 8.3.0 — Pillow (PIL Fork) 8.3.0 documentation | MISC | pillow.readthedc |
| [SECURITY] [DLA 2716-1] pillow security update | MLIST | lists.debian.org |
| CVE Program record | CVE.ORG | www.cve.org |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 178719 Debian Security Update for pillow (DLA 2716-1) |
| 179653 Debian Security Update for pillow (CVE-2021-34552) |
| 198632 Ubuntu Security Notification for Pillow Vulnerabilities (USN-5227-1) |
| 239802 Red Hat Update for python-pillow (RHSA-2021:4149) |
| 239895 Red Hat Update for Satellite 6.10 (RHSA-2021:4702) |
| 281759 Fedora Security Update for mingw (FEDORA-2021-3ec845dc0c) |
| 281760 Fedora Security Update for mingw (FEDORA-2021-bf01a738f3) |
| 296060 Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021) |
| 355121 Amazon Linux Security Advisory for python-pillow : ALAS2023-2023-146 |
| 355393 Amazon Linux Security Advisory for python-pillow : ALAS2-2023-2083 |
| 375694 Python Pillow Library Buffer Overflow Vulnerability |
| 377325 Alibaba Cloud Linux Security Update for python-pillow (ALINUX3-SA-2022:0012) |
| 502016 Alpine Linux Security Update for py3-pillow |
| 505318 Alpine Linux Security Update for py3-pillow |
| 670723 EulerOS Security Update for python-pillow (EulerOS-SA-2021-2481) |
| 670760 EulerOS Security Update for python-pillow (EulerOS-SA-2021-2518) |
| 670782 EulerOS Security Update for python-pillow (EulerOS-SA-2021-2540) |
| 670806 EulerOS Security Update for python-pillow (EulerOS-SA-2021-2564) |
| 670990 EulerOS Security Update for python-pillow (EulerOS-SA-2021-2611) |
| 710682 Gentoo Linux Pillow Multiple Vulnerabilities (GLSA 202211-10) |
| 750950 OpenSUSE Security Update for python-CairoSVG, python-Pillow (openSUSE-SU-2021:1134-1) |
| 940109 AlmaLinux Security Update for python-pillow (ALSA-2021:4149) |
| 960087 Rocky Linux Security Update for python-pillow (RLSA-2021:4149) |
| 980520 Python (pip) Security Update for pillow (GHSA-7534-mm45-c74v) |

© [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](#)