

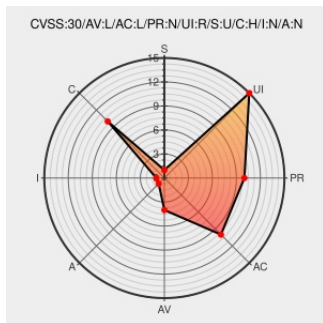


CVE-2016-9189

Published on: 11/04/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

CVE-2016-9189

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Pillow before 3.3.2 allows context-dependent attackers to obtain sensitive information by using the "crafted image file" approach, related to an "Integer Overflow" issue affecting the Image.core.map_buffer in map.c component.

CVE-2016-9189 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Fixes for #2105 by wiredfool · Pull Request #2146 · python-pillow/Pillow · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/python-pillow/Pillow/pull/2146/commits/c50ebe6459a131a1ea8ca531f10da616d3ceaa0f

Python Pillow Multiple Security Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94234
Debian -- Security Information -- DSA-3710-1 pillow	Third Party Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-3710
Multiple memory corruption vulnerabilities · Issue #2105 · python-pillow/Pillow · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/python-pillow/Pillow/issues/2105
3.3.2 — Pillow (PIL Fork) 3.4.2 documentation	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM pillow.readthedocs.io/en/3.4.x/releasesnotes/3.3.2.html
Pillow: Multiple vulnerabilities (GLSA 201612-52) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201612-52
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

Related QID Numbers

[980868](#) Python (pip) Security Update for Pillow (GHSA-rwr3-c2q8-gm56)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Python	Pillow	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:python:pillow:*****:						

© [CVE.report](#) 2023   |

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](#)