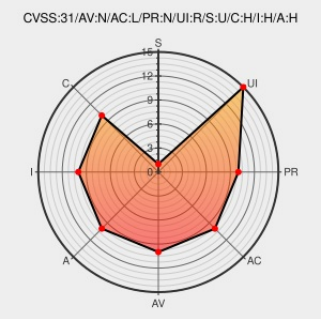
CVE-2017-16546

Published on: 11/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16546

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The ReadWPGImage function in coders/wpg.c in ImageMagick 7.0.7-9 does not properly validate the colormap index in a WPG palette, which allows remote attackers to cause a denial of service (use of uninitialized data or invalid memory allocation) or possibly have unspecified other impact via a malformed WPG file.

CVE-2017-16546 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
https://github.com/ImageMagick/ImageMagick/issues/851 · ImageMagick/ImageMagick@e04cf3e · GitHub	Issue Tracking, Third Party Advisory, github.com	CONFIRM github.com/ImageMagick/ImageMagick/commit/e04cf3e952

	text/html	
Debian -- Security Information -- DSA-4040-1 imagemagick	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4040
Debian -- Security Information -- DSA-4074-1 imagemagick	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4074
https://github.com/ImageMagick/ImageMagick/issues/85 · ImageMagick/ImageMagick@2130bf6 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/commit/2130bf6f89c
USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3681-1
Heap Allocation errors, uninitialized integers used to allocate memory as well as conditional jumps depending on uninitialized values, while feeding a malformed WPG File · Issue #851 · ImageMagick/ImageMagick · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/issues

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-9	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-9	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.7-9:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.7-9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→