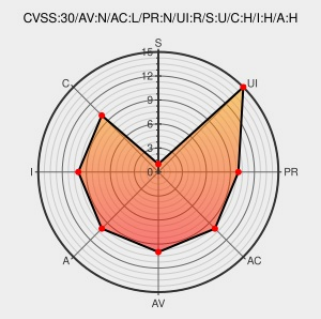
CVE-2014-9831

Published on: 08/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9831

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



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file.

CVE-2014-9831 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
oss-security - Re: ImageMagick CVEs	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160602 Re: ImageMagick CVEs

404 Not Found	Issue Tracking Patch Third Party Advisory anonscm.debian.org text/html Inactive Link Not Archived	CONFIRM anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=b68b78e2625122d9f6b6d88ba4df7e85b47b556f
1343487 – (CVE-2014-9831) CVE-2014-9831 ImageMagick: handling of corrupted wpg file	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1343487

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	All	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→