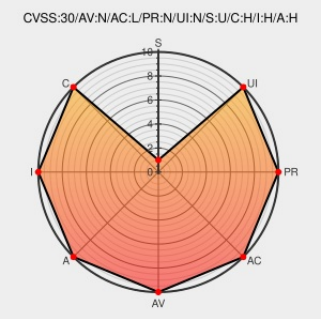
CVE-2015-8871

Published on: 09/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8871

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Use-after-free vulnerability in the opj_j2k_write_mco function in j2k.c in OpenJPEG before 2.1.1 allows remote attackers to have unspecified impact via unknown vectors.

CVE-2015-8871 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
OpenJPEG: Multiple vulnerabilities (GLSA 201612-26) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201612-26
oss-security - Re: CVE	Mailing List	MLIST [oss-security] 20160512 Re: CVE Request : Use-after-free in openjpeg

Request : Use-after-free in openjpeg	Third Party Advisory www.openwall.com text/html	
Use-after-free in opj_j2k_write_mco · Issue #563 · uclouvain/openjpeg · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/uclouvain/openjpeg/issues/563
Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let Local Apps Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1038623
Bug 1263359 – openjpeg: Use-after-free vulnerability in opj_j2k_write_mco	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1263359
Debian -- Security Information -- DSA-3665-1 openjpeg2	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3665
Fix potential use-after-free in opj_j2k_write_mco function · uclouvain/openjpeg@940100c · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/uclouvain/openjpeg/commit/940100c28ae2893172229079488 9cf84a92
oss-security - CVE Request : Use-after-free in openjpeg	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20150915 CVE Request : Use-after-free in openjpeg
openjpeg/CHANGELOG.md at master · uclouvain/openjpeg · GitHub	Release Notes Third Party Advisory github.com text/html	CONFIRM github.com/uclouvain/openjpeg/blob/master/CHANGELOG.md

There are currently no QIDs associated with this CVE

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	Uclouvain	Openjpeg	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:uclouvain:openjpeg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→