



CVE-2012-2806

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

Summary

CVE	CVE-2012-2806
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-13 20:55:00 UTC
Updated	2023-12-20 18:28:00 UTC
Description	Heap-based buffer overflow in the get_sos function in jdmarker.c in libjpeg-turbo 1.2.0 allows remote attackers to cause a d

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D.r.commander	Libjpeg-turbo	1.2.0	All	All	All
Application	D.r.commander	Libjpeg-turbo	1.2.0	All	All	All

References

Reference	Source	Link
Security Advisory SA50753 - Gentoo update for libjpeg-turbo - Secunia		secunia.
Bug 826849 – CVE-2012-2806 libjpeg-turbo: Heap-based buffer overflow when decompressing corrupt JPEG images	MISC	bugzilla.
Security Alerts - Secunia	SECUNIA	secunia.
759802 – (CVE-2012-2806) Null-pointer execution/null out of bounds write at libjpeg/jdmarker.c	MISC	bugzilla.
oss-security - libjpeg-turbo: Heap-based buffer overflow when decompressing corrupt JPEG images	MLIST	www.op
Support / Security / Advisories / / MDVSA-2012:121 Mandriva		www.ma
libjpeg-turbo Heap-Based Buffer Overflow Vulnerability	BID	www.sec
IBM X-Force Exchange	XF	exchang
84040		osvdb.or
Gentoo Linux Documentation -- libjpeg-turbo: User-assisted execution of arbitrary code		security.
404 Not Found	CONFIRM	libjpeg-t
CVE Program record	CVE.ORG	www.cve

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report