



# CVE-2007-2833

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

## Summary

<b>CVE</b>	CVE-2007-2833
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-06-21 20:30:00 UTC
<b>Updated</b>	2008-09-05 21:24:00 UTC
<b>Description</b>	Emacs 21 allows user-assisted attackers to cause a denial of service (crash) via certain crafted images, as demonstrated v

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-32	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	sparc	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007.1	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007.1	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	x86_64	All

## References

Reference	Source	Link	Tags
USN-504-1: Emacs vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>	
Debian -- Security Information -- DSA-1316-1 emacs21	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
#408929 - emacs21: crash on spam - Debian Bug report logs	CONFIRM	<a href="http://bugs.debian.org">bugs.debian.org</a>	
GNU Emacs Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	
Advisories - Mandriva Linux	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>	
GNU Emacs Image Processing Remote Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
issues.rpath.com/browse/RPL-1490	CONFIRM	<a href="http://issues.rpath.com">issues.rpath.com</a>	

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-06-26	Mark J Cox	Red Hat does not consider a user-assisted crash of a user application such as Emacs to be a se

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

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**