



# CVE-2008-0411

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

## Summary

<b>CVE</b>	CVE-2008-0411
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-02-28 21:44:00 UTC
<b>Updated</b>	2018-10-15 21:59:00 UTC
<b>Description</b>	Stack-based buffer overflow in the zseticcspace function in zicc.c in Ghostscript 8.61 and earlier allows remote attackers to

## Risk And Classification

### Problem Types: CWE-119

## 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>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	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
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	All	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="#">Ghostscript</a>	<a href="#">Ghostscript</a>	0	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	8.0.1	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	8.15	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	0	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	8.0.1	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	8.15	All	All	All
Application	<a href="#">Ghostscript</a>	<a href="#">Ghostscript</a>	All	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrakesoft Corporate Server</a>	3.0_x86_64	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrakesoft Corporate Server</a>	4.0_x86_64	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrakesoft Corporate Server</a>	3.0_x86_64	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrakesoft Corporate Server</a>	4.0_x86_64	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>	2007.0_x86_64	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007.1	All	All	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>	2008.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2008.0	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>	2007.0_x86_64	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2007.1	All	All	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>	2008.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2008.0	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>	4.0	All	All	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>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5	All	server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	as_3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	as_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	es_3	All	All	All

Operating System	<a href="#">Hedhat</a>	<a href="#">Enterprise Linux</a>	es_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	ws_3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	ws_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5	All	server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	as_3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	as_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	es_3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	es_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	ws_3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	ws_4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5	All	client	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	5	All	client	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Workstation</a>	5	All	client	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Workstation</a>	5	All	client	All
Operating System	<a href="#">Rpath</a>	<a href="#">Rpath Linux</a>	1	All	All	All
Operating System	<a href="#">Rpath</a>	<a href="#">Rpath Linux</a>	1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Novell Linux Pos</a>	9	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Novell Linux Pos</a>	9	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Open Suse</a>	10.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Open Suse</a>	10.3	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Open Suse</a>	10.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Open Suse</a>	10.3	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10	sp1	enterprise_desktop	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10	sp1	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	ppc	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	x86	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10	sp1	enterprise_desktop	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10	sp1	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	ppc	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	x86	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	10.1	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	enterprise_server	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Open Enterprise Server</a>	0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Open Enterprise Server</a>	0	All	All	All

## References

Reference	Source	Li
<a href="#">CESA-2008-001 - rev 2</a>	MISC	sc
<a href="#">Ghostscript "zseticcspace()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com</a>	SECUNIA	se
<a href="#">Ubuntu update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">[SECURITY] Fedora 8 Update: ghostscript-8.61-8.fc8</a>	FEDORA	w
<a href="#">Gentoo update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">USN-599-1: Ghostscript vulnerability   Ubuntu</a>	UBUNTU	w
<a href="#">Debian update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">SecurityFocus</a>	BUGTRAQ	w
<a href="#">Webmail : Solution de messagerie professionnelle - OVHcloud- OVH</a>	VUPEN	w
<a href="#">Ghostscript zseticcspace() Function Buffer Overflow Vulnerability</a>	BID	w
<a href="#">Support / Security / Advisories // MDVSA-2008:055   Mandriva</a>	MANDRIVA	w
<a href="#">Ghostscript: Buffer overflow — Gentoo Linux Documentation</a>	GENTOO	w
<a href="#">Red Hat update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">Repository / Oval Repository</a>	OVAL	ov
<a href="#">Mandriva update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">rPath update for espgs - Advisories - Secunia</a>	SECUNIA	se
<a href="#">rhn.redhat.com   Red Hat Support</a>	REDHAT	w
<a href="#">The Slackware Linux Project: Slackware Security Advisories</a>	SLACKWARE	sl
<a href="#">Debian -- Security Information -- DSA-1510-1 ghostscript</a>	DEBIAN	w
<a href="#">[security-announce] SUSE Security Announcement: ghostscript (SUSE-SA:200</a>	SUSE	lis
<a href="#">SecurityFocus</a>	BUGTRAQ	w
<a href="#">Slackware update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">Ghostscript Stack Overflow in zseticcspace() Lets Remote Users Execute Arbitrary Codes - SecurityTracker</a>	SECTRACK	w
<a href="#">Advisories:rPSA-2008-0082 - rPath Wiki</a>	CONFIRM	wi
<a href="#">issues.rpath.com/browse/RPL-2217</a>	CONFIRM	is
<a href="#">SUSE update for ghostscript - Secunia Advisories - Vulnerability Intelligence - Secunia.com</a>	SECUNIA	se
<a href="#">Fedora update for ghostscript - Advisories - Secunia</a>	SECUNIA	se
<a href="#">CVE Program record</a>	CVE.ORG	w
<a href="#">NVD vulnerability detail</a>	NVD	nv

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)