



# CVE-2004-1005

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

## Summary

<b>CVE</b>	CVE-2004-1005
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-04-14 04:00:00 UTC
<b>Updated</b>	2017-07-11 01:30:00 UTC
<b>Description</b>	Multiple buffer overflows in Midnight Commander (mc) 4.5.55 and earlier allow remote attackers to have an unknown impact

## 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>	3.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.40	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.41	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.42	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.43	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.44	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.45	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.46	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.47	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.48	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.49	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.50	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.51	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.52	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.54	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.55	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.6	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.40	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.41	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.42	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.43	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.44	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.45	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.46	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.47	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.48	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.49	All	All	All

Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.50	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.51	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.52	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.54	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.55	All	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	advanced_server_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	2.1	All	workstation_ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium_processor	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	ia64	All
Operating System	<a href="#">Redhat</a>	<a href="#">Linux Advanced Workstation</a>	2.1	All	itanium_processor	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Server</a>	7.0	All	All	All

Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Server</a>	8.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Server</a>	7.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Server</a>	8.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Workstation</a>	8.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Turbolinux</a>	<a href="#">Turbolinux Workstation</a>	8.0	All	All	All

## References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Debian -- Security Information -- DSA-639-1 mc	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
<a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	Patch, Vendor
Secunia - Advisories - Debian update for mc	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Patch, Vendor
Gentoo Linux Documentation -- Midnight Commander: Multiple vulnerabilities	GENTOO	<a href="https://www.gentoo.org">www.gentoo.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

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](https://status.cve.report)