



# CVE-2004-0232

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

## Summary

<b>CVE</b>	CVE-2004-0232
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-08-18 04:00:00 UTC
<b>Updated</b>	2017-07-11 01:29:00 UTC
<b>Description</b>	Multiple format string vulnerabilities in Midnight Commander (mc) before 4.6.0 may allow attackers to cause a denial of serv

## 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="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Application	<a href="#">Midnight Commander</a>	<a href="#">Midnight Commander</a>	4.5.40	All	All	All



Operating System	<a href="#">Slackware</a>	<a href="#">Slackware Linux</a>	9.1	All	All	All
Operating System	<a href="#">Slackware</a>	<a href="#">Slackware Linux</a>	All	All	All	All
Operating System	<a href="#">Slackware</a>	<a href="#">Slackware Linux</a>	9.0	All	All	All
Operating System	<a href="#">Slackware</a>	<a href="#">Slackware Linux</a>	9.1	All	All	All

## References

Reference	Source	Link	Tags
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
Gentoo Linux Documentation -- Midnight Commander: Multiple vulnerabilities	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
Debian -- Security Information -- DSA-497-1 mc	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.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, ar

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)