



CVE-2010-0296

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

Summary

CVE	CVE-2010-0296
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-01 20:30:00 UTC
Updated	2023-02-13 02:21:00 UTC
Description	The encode_name macro in misc/mntent_r.c in the GNU C Library (aka glibc or libc6) 2.11.1 and earlier, as used by ncpmo

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.10	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.2	All	All	All

Application	Gnu	Glibc	2.2.1	All	All	All
Application	Gnu	Glibc	2.2.2	All	All	All
Application	Gnu	Glibc	2.2.3	All	All	All
Application	Gnu	Glibc	2.2.4	All	All	All
Application	Gnu	Glibc	2.2.5	All	All	All
Application	Gnu	Glibc	2.3	All	All	All
Application	Gnu	Glibc	2.3.1	All	All	All
Application	Gnu	Glibc	2.3.10	All	All	All
Application	Gnu	Glibc	2.3.2	All	All	All
Application	Gnu	Glibc	2.3.3	All	All	All
Application	Gnu	Glibc	2.3.4	All	All	All
Application	Gnu	Glibc	2.3.5	All	All	All
Application	Gnu	Glibc	2.3.6	All	All	All
Application	Gnu	Glibc	2.4	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.5.1	All	All	All
Application	Gnu	Glibc	2.6	All	All	All
Application	Gnu	Glibc	2.6.1	All	All	All
Application	Gnu	Glibc	2.7	All	All	All
Application	Gnu	Glibc	2.8	All	All	All
Application	Gnu	Glibc	2.9	All	All	All
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.10	All	All	All

Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.2	All	All	All
Application	Gnu	Glibc	2.2.1	All	All	All
Application	Gnu	Glibc	2.2.2	All	All	All
Application	Gnu	Glibc	2.2.3	All	All	All
Application	Gnu	Glibc	2.2.4	All	All	All
Application	Gnu	Glibc	2.2.5	All	All	All
Application	Gnu	Glibc	2.3	All	All	All
Application	Gnu	Glibc	2.3.1	All	All	All
Application	Gnu	Glibc	2.3.10	All	All	All
Application	Gnu	Glibc	2.3.2	All	All	All
Application	Gnu	Glibc	2.3.3	All	All	All
Application	Gnu	Glibc	2.3.4	All	All	All
Application	Gnu	Glibc	2.3.5	All	All	All
Application	Gnu	Glibc	2.3.6	All	All	All
Application	Gnu	Glibc	2.4	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.5.1	All	All	All
Application	Gnu	Glibc	2.6	All	All	All
Application	Gnu	Glibc	2.6.1	All	All	All
Application	Gnu	Glibc	2.7	All	All	All
Application	Gnu	Glibc	2.8	All	All	All
Application	Gnu	Glibc	2.9	All	All	All
Application	Gnu	Glibc	All	All	All	All

References						
Reference						Source
Full Disclosure: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series						FULLDISCLOSURE
Support						REDHAT
Ubuntu update for glibc and eglibc - Advisories - Community						SECURITY
Bugtraq: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series						BUGTRAQ
Gentoo Linux Documentation -- GNU C library: Multiple vulnerabilities						GENTOO
SecurityFocus						BUGTRAQ
sourceware.org Git - glibc.git/commit						CONFIRMATION
Debian -- Security Information -- DSA-2058-1 glibc, eglibc						DEBIAN

Red Hat update for glibc - Secunia.com	SECUNIA
Bug 559579 – CVE-2010-0296 glibc: Improper encoding of names with certain special character in utilities for writing to mtab table	CONFIRMED
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Support / Security / Advisories // MDVSA-2010:111 Mandriva	MANDRIVA
Support / Security / Advisories // MDVSA-2010:112 Mandriva	MANDRIVA
IBM X-Force Exchange	XF
SecurityTracker.com Archives - GNU Glibc mntent Newline Processing Error Lets Local Users Gain Elevated Privileges	SECURITYTRACKER
Frugalware Linux - Let's make things Frugal!	CONFIRMED
VMSA-2011-0012.2	CONFIRMED
USN-944-1: GNU C Library vulnerabilities Ubuntu	UBUNTU
About Secunia Research Flexera	SECUNIA
sourceware.org Git - glibc.git/commit	MISC
[security-announce] SUSE Security Announcement: glibc (SUSE-SA:2010:052)	SUSE
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
WAGO 852 Industrial Managed Switch Series Code Execution / Hardcoded Credentials ≈ Packet Storm	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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](#).

Free CVE JSON API [cve.report/api](#)

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