



CVE-2011-1095

Published on: 04/09/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:15:00 AM UTC

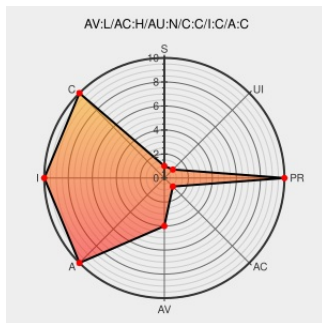
CVE-2011-1095

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Glibc](#) from [Gnu](#) contain the following vulnerability: locale/programs/locale.c in locale in the GNU C Library (aka glibc or libc6) before 2.13 does not quote its output, which might allow local users to gain privileges via a crafted localization environment variable, in conjunction with a program that executes a script that uses the eval function.

CVE-2011-1095 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.2 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

LOCAL

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Support

www.redhat.com
text/html

[REDHAT RHSA-2011:0412](#)

oss-security - glibc locale
escaping issue

Exploit
Patch
openwall.com
text/html

[MLIST \[oss-security\] 20110308 glibc locale escaping issue](#)

Glibc Locale Command May
Let Local Users Gain
Elevated Privileges -
SecurityTracker

securitytracker.com
text/html

[SECTRAK 1025286](#)

Gentoo Linux
Documentation -- GNU C
library: Multiple
vulnerabilities

Vendor Advisory
security.gentoo.org
text/html

[GENTOO GLSA-201011-01](#)

oss-security - Re: glibc locale escaping issue	Exploit Patch openwall.com text/html	 MLIST [oss-security] 20110308 Re: glibc locale escaping issue
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20111013 VMSA-2011-0012 VMware ESXi and ESX updates to third party libraries and ESX Service Console
11904 – (CVE-2011-1095) locale command does not quote (invalid) locale strings (CVE-2011-1095)	Exploit sourceware.org text/html	 CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=11904
Red Hat update for glibc - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 43830
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2011-0863
11904 – (CVE-2011-1095) locale command does not quote (invalid) locale strings (CVE-2011-1095)	Exploit sources.redhat.com text/html	 CONFIRM sources.redhat.com/bugzilla/show_bug.cgi?id=11904
Security Advisories Mandriva Linux	www.mandriva.com text/html	 MANDRIVA MDVSA-2011:178
VMSA-2011-0012.2	www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2011-0012.html
625893 – (CVE-2011-1095) CVE-2011-1095 glibc: insufficient quoting in the locale command output	Exploit Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=625893
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:12272
About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 46397
sourceware.org Git	Patch sourceware.org text/x-diff Inactive Link Not Archived	 MISC sourceware.org/git/?p=glibc.git%3Ba=patch%3Bh=026373745eab50a683536d950cb7e17dc98c4259
Gentoo Bug 330923 -	Exploit Patch bugs.gentoo.org text/html	 CONFIRM bugs.gentoo.org/show_bug.cgi?id=330923
oss-security - Re: glibc locale escaping issue	openwall.com text/html	 MLIST [oss-security] 20110308 Re: glibc locale escaping issue
Support	www.redhat.com text/html	 REDHAT RHSA-2011:0413
GNU C Library "locale" Quoting Weakness - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 43976
Red Hat update for glibc - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 43989

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	1.00	All	All	All
Application	Gnu	Glibc	1.01	All	All	All
Application	Gnu	Glibc	1.02	All	All	All
Application	Gnu	Glibc	1.03	All	All	All
Application	Gnu	Glibc	1.04	All	All	All
Application	Gnu	Glibc	1.05	All	All	All
Application	Gnu	Glibc	1.06	All	All	All
Application	Gnu	Glibc	1.07	All	All	All
Application	Gnu	Glibc	1.08	All	All	All
Application	Gnu	Glibc	1.09	All	All	All
Application	Gnu	Glibc	1.09.1	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	2.1.3.10	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	2.10.2	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12.0	All	All	All
Application	Gnu	Glibc	2.12.1	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	1.00	All	All	All
Application	Gnu	Glibc	1.01	All	All	All
Application	Gnu	Glibc	1.02	All	All	All
Application	Gnu	Glibc	1.03	All	All	All
Application	Gnu	Glibc	1.04	All	All	All
Application	Gnu	Glibc	1.05	All	All	All
Application	Gnu	Glibc	1.06	All	All	All

Application	Gnu	Glibc	1.06	All	All	All
Application	Gnu	Glibc	1.07	All	All	All
Application	Gnu	Glibc	1.08	All	All	All
Application	Gnu	Glibc	1.09	All	All	All
Application	Gnu	Glibc	1.09.1	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	2.1.3.10	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	2.10.2	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12.0	All	All	All
Application	Gnu	Glibc	2.12.1	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
cpe:2.3:a:gnu:glibc:1.00:*****:						
cpe:2.3:a:gnu:glibc:1.01:*****:						
cpe:2.3:a:gnu:glibc:1.02:*****:						
cpe:2.3:a:gnu:glibc:1.03:*****:						
cpe:2.3:a:gnu:glibc:1.04:*****:						
cpe:2.3:a:gnu:glibc:1.05:*****:						
cpe:2.3:a:gnu:glibc:1.06:*****:						
cpe:2.3:a:gnu:glibc:1.07:*****:						
cpe:2.3:a:gnu:glibc:1.08:*****:						
cpe:2.3:a:gnu:glibc:1.09:*****:						
cpe:2.3:a:gnu:glibc:1.09.1:*****:						
cpe:2.3:a:gnu:glibc:2.0:*****:						
cpe:2.3:a:gnu:glibc:2.0.1:*****:						
cpe:2.3:a:gnu:glibc:2.0.2:*****:						
cpe:2.3:a:gnu:glibc:2.0.3:*****:						
cpe:2.3:a:gnu:glibc:2.0.4:*****:						

cpe:2.3:a:gnu:glibc:2.0.5:****:
cpe:2.3:a:gnu:glibc:2.0.6:****:
cpe:2.3:a:gnu:glibc:2.1:****:
cpe:2.3:a:gnu:glibc:2.1.1:****:
cpe:2.3:a:gnu:glibc:2.1.1.6:****:
cpe:2.3:a:gnu:glibc:2.1.2:****:
cpe:2.3:a:gnu:glibc:2.1.3:****:
cpe:2.3:a:gnu:glibc:2.1.3.10:****:
cpe:2.3:a:gnu:glibc:2.1.9:****:
cpe:2.3:a:gnu:glibc:2.10:****:
cpe:2.3:a:gnu:glibc:2.10.1:****:
cpe:2.3:a:gnu:glibc:2.10.2:****:
cpe:2.3:a:gnu:glibc:2.11:****:
cpe:2.3:a:gnu:glibc:2.11.1:****:
cpe:2.3:a:gnu:glibc:2.11.2:****:
cpe:2.3:a:gnu:glibc:2.11.3:****:
cpe:2.3:a:gnu:glibc:2.12.0:****:
cpe:2.3:a:gnu:glibc:2.12.1:****:
cpe:2.3:a:gnu:glibc:2.2:****:
cpe:2.3:a:gnu:glibc:2.2.1:****:
cpe:2.3:a:gnu:glibc:2.2.2:****:
cpe:2.3:a:gnu:glibc:2.2.3:****:
cpe:2.3:a:gnu:glibc:2.2.4:****:
cpe:2.3:a:gnu:glibc:2.2.5:****:
cpe:2.3:a:gnu:glibc:2.3:****:
cpe:2.3:a:gnu:glibc:2.3.1:****:
cpe:2.3:a:gnu:glibc:2.3.10:****:
cpe:2.3:a:gnu:glibc:2.3.2:****:
cpe:2.3:a:gnu:glibc:2.3.3:****:

cpe:2.3:a:gnu:glibc:2.3:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.3.4:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.3.5:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.3.6:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.4:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.5:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.5.1:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.6:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.6.1:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.7:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.8:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.9:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.00:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.01:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.02:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.03:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.04:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.05:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.06:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.07:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.08:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.09:*.***:*.***:*
cpe:2.3:a:gnu:glibc:1.09.1:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0.1:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0.2:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0.3:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0.4:*.***:*.***:*
cpe:2.3:a:gnu:glibc:2.0.5:*.***:*.***:*

cpe:2.3:a:gnu:glibc:2.0.6:****:
cpe:2.3:a:gnu:glibc:2.1:****:
cpe:2.3:a:gnu:glibc:2.1.1:****:
cpe:2.3:a:gnu:glibc:2.1.1.6:****:
cpe:2.3:a:gnu:glibc:2.1.2:****:
cpe:2.3:a:gnu:glibc:2.1.3:****:
cpe:2.3:a:gnu:glibc:2.1.3.10:****:
cpe:2.3:a:gnu:glibc:2.1.9:****:
cpe:2.3:a:gnu:glibc:2.10:****:
cpe:2.3:a:gnu:glibc:2.10.1:****:
cpe:2.3:a:gnu:glibc:2.10.2:****:
cpe:2.3:a:gnu:glibc:2.11:****:
cpe:2.3:a:gnu:glibc:2.11.1:****:
cpe:2.3:a:gnu:glibc:2.11.2:****:
cpe:2.3:a:gnu:glibc:2.11.3:****:
cpe:2.3:a:gnu:glibc:2.12.0:****:
cpe:2.3:a:gnu:glibc:2.12.1:****:
cpe:2.3:a:gnu:glibc:2.2:****:
cpe:2.3:a:gnu:glibc:2.2.1:****:
cpe:2.3:a:gnu:glibc:2.2.2:****:
cpe:2.3:a:gnu:glibc:2.2.3:****:
cpe:2.3:a:gnu:glibc:2.2.4:****:
cpe:2.3:a:gnu:glibc:2.2.5:****:
cpe:2.3:a:gnu:glibc:2.3:****:
cpe:2.3:a:gnu:glibc:2.3.1:****:
cpe:2.3:a:gnu:glibc:2.3.10:****:
cpe:2.3:a:gnu:glibc:2.3.2:****:
cpe:2.3:a:gnu:glibc:2.3.3:****:
cpe:2.3:a:gnu:glibc:2.3.4:****:

cpe:2.3:a:gnu:glibc:2.3.4:*****:
cpe:2.3:a:gnu:glibc:2.3.5:*****:
cpe:2.3:a:gnu:glibc:2.3.6:*****:
cpe:2.3:a:gnu:glibc:2.4:*****:
cpe:2.3:a:gnu:glibc:2.5:*****:
cpe:2.3:a:gnu:glibc:2.5.1:*****:
cpe:2.3:a:gnu:glibc:2.6:*****:
cpe:2.3:a:gnu:glibc:2.6.1:*****:
cpe:2.3:a:gnu:glibc:2.7:*****:
cpe:2.3:a:gnu:glibc:2.8:*****:
cpe:2.3:a:gnu:glibc:2.9:*****:
cpe:2.3:a:gnu:glibc:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)