

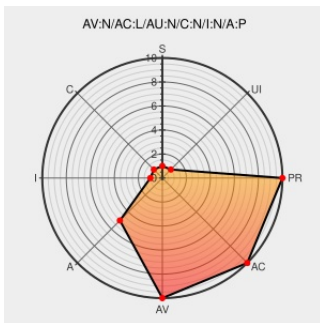


CVE-2012-3405

Published on: 02/10/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:23 AM UTC

CVE-2012-3405

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The `vfprintf` function in `stdio-common/vfprintf.c` in `libc` in GNU C Library (aka `glibc`) 2.14 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the `FORTIFY_SOURCE` format-string protection mechanism and cause a denial of service (segmentation fault and crash) via a format string with

a large number of format specifiers that triggers "desynchronization within the buffer size handling," a different vulnerability than CVE-2012-3404.

CVE-2012-3405 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

USN-1589-1: GNU C Library vulnerabilities | Ubuntu

www.ubuntu.com

text/html

[UBUNTU USN-1589-1](#)

oss-security - Re: CVE request: glibc formatted printing vulnerabilities

www.openwall.com

text/html

[MLIST \[oss-security\] 20120711 Re: CVE request: glibc formatted printing vulnerabilities](#)

Red Hat Customer Portal

web.archive.org

text/html

Inactive Link Not Archived

[REDHAT RHSA-2012:1098](#)

13446 – (CVE-2012-3405) crash in `vfprintf` with more than 64 format

sourceware.org

[CONFIRM](#)

args and format specifiers (CVE-2012-3405)	text/html	sourceware.org/bugzilla/show_bug.cgi?id=13446
Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201503-04
833704 – (CVE-2012-3405) CVE-2012-3405 glibc: incorrect use of extend_alloca() in formatted printing can lead to FORTIFY_SOURCE format string protection bypass	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=833704
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:1200

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
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	8.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	10.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	Its	All
Operating System	Canonical	Ubuntu Linux	8.04	-	Its	All
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

Application	Redhat	Enterprise Virtualization	3.0	All	All	All
Application	Redhat	Enterprise Virtualization	3.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:-:lts:*:*:*:*:						
cpe:2.3:a:gnu:glibc:2.14:*:*:*:*:*:						
cpe:2.3:a:gnu:glibc:2.14:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:						
cpe:2.3:a:redhat:enterprise_virtualization:3.0:*:*:*:*:*:						
cpe:2.3:a:redhat:enterprise_virtualization:3.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)