CVE-2012-3406

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2012-3406
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-10 18:15:00 UTC
Updated	2019-04-22 17:48:00 UTC
Description	The vfprintf function in stdio-common/vfprintf.c in GNU C Library (aka glibc) 2.5, 2.12, and probably other versions does not

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	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	-	lts	All
Operating System	Canonical	Ubuntu Linux	8.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	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	-	lts	All
Operating System	Canonical	Ubuntu Linux	8.04	-	lts	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.5	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	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

References

Reference	Source	Lir
Red Hat Customer Portal	REDHAT	rhn
USN-1589-1: GNU C Library vulnerabilities | Ubuntu	UBUNTU	ww
oss-security - Re: CVE request: glibc formatted printing vulnerabilities	MLIST	ww
Red Hat Customer Portal	REDHAT	rhn
bugzilla.redhat.com/attachment.cgi	CONFIRM	bug
Red Hat Customer Portal	REDHAT	rhn
Gentoo Security	GENTOO	sec
Bug 826943 – CVE-2012-3406 glibc: printf() unbound alloca() usage in case of positional parameters + many format specs	CONFIRM	bug
Red Hat Customer Portal	REDHAT	rhn
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.