CVE-2012-0864

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-0864
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-02 14:55:00 UTC
Updated	2023-02-13 03:28:00 UTC
Description	Integer overflow in the vfprintf function in stdio-common/vfprintf.c in glibc 2.14 and other versions allows context-dependent

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redh
Red Hat Customer Portal	REDHAT	rhn.redh
GNU glibc 'nargs' Integer Overflow Security Bypass Vulnerability	BID	www.se
Red Hat Customer Portal	MISC	access.r
Red Hat Customer Portal	MISC	access.r
sourceware.org Git - glibc.git/commitdiff	MISC	sourcew
.:: Phrack Magazine ::.	MISC	www.ph
access.redhat.com | CVE-2012-0864	MISC	access.r
Red Hat Customer Portal	REDHAT	rhn.redh
Bug 794766 – CVE-2012-0864 glibc: FORTIFY_SOURCE format string protection bypass via "nargs" integer overflow	CONFIRM	bugzilla.
Kees Cook - [PATCH] vfprintf: validate nargs and positional offsets	MLIST	sourcew
Red Hat Customer Portal	MISC	access.r

sourceware.org Git - glibc.git/commitdiff	MISC	sourcew
Red Hat Customer Portal	REDHAT	rhn.redh
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.r
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

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