



CVE-2011-0536

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

Summary

CVE	CVE-2011-0536
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-08 15:17:00 UTC
Updated	2023-02-13 01:18:00 UTC
Description	Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc o

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.12-1.7.el6_0.3	All	All	All
Application	Gnu	Glibc	2.5-49.el5_5.6	All	All	All
Application	Gnu	Glibc	2.12-1.7.el6_0.3	All	All	All
Application	Gnu	Glibc	2.5-49.el5_5.6	All	All	All
Operating System	Redhat	Enterprise Linux	All	All	All	All
Operating System	Redhat	Enterprise Linux	All	All	All	All

References

Reference
Support
sourceware.org Git - glibc.git/commit
SecurityFocus
Repository / Oval Repository
Red Hat Customer Portal
[SECURITY] [DSA 2122-2] New glibc packages fix privilege escalation
oss-security - Re: CVE request: glibc CVE-2010-3847 fix regression
Red Hat update for glibc - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Red Hat Customer Portal
Security Advisories Mandriva Linux
VMSA-2011-0012.2
access.redhat.com CVE-2011-0536
About Secunia Research Flexera
Bug #701783 "iconv libraries not loading" : Bugs : glibc package : Ubuntu
sourceware.org Git - glibc.git/commit
Support
oss-security - CVE request: glibc CVE-2010-3847 fix regression
Glibc Regression Lets Local Users Gain Elevated Privileges - SecurityTracker
667974 – (CVE-2011-0536) CVE-2011-0536 glibc: CVE-2010-3847 fix causes linker to search CWD when running privileged program with \$C
USN-1009-2: GNU C Library vulnerability Ubuntu
Red Hat update for glibc - Secunia.com
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.