CVE-2017-16997

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

Summary

CVE	CVE-2017-16997
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-18 01:29:00 UTC
Updated	2020-10-15 13:28:00 UTC
Description	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $OR

Risk And Classification

Problem Types: CWE-426

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.19	All	All	All
Application	Gnu	Glibc	2.20	All	All	All
Application	Gnu	Glibc	2.21	All	All	All
Application	Gnu	Glibc	2.22	All	All	All
Application	Gnu	Glibc	2.23	All	All	All
Application	Gnu	Glibc	2.25	All	All	All
Application	Gnu	Glibc	2.26	All	All	All
Application	Gnu	Glibc	2.19	All	All	All
Application	Gnu	Glibc	2.20	All	All	All
Application	Gnu	Glibc	2.21	All	All	All
Application	Gnu	Glibc	2.22	All	All	All
Application	Gnu	Glibc	2.23	All	All	All
Application	Gnu	Glibc	2.25	All	All	All
Application	Gnu	Glibc	2.26	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference
22625 – (CVE-2017-16997) RPATH $ORIGIN replaced by PWD for AT_SECURE/SUID binaries or if /proc is not mounted (CVE-2017-16997)
Red Hat Customer Portal
GNU C Library 'elf/dl-load.c ' CVE-2017-16997 Local Privilege Escalation Vulnerability
#884615 - src:glibc: CVE-2017-16997: incorrect RPATH/RUNPATH handling for SUID binaries - Debian Bug report logs
Aurelien Jarno - [PATCH] elf: Check for empty tokens before dynamic string token expansio
Red Hat Customer Portal
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.