CVE-2017-1000366

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-1000366
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-19 16:29:00 UTC
Updated	2020-10-15 13:28:00 UTC
Description	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp2	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp2	All	All
Operating System	Novell	Suse Linux Enterprise Point Of Sale	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Point Of Sale	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp3	All	All
Application	Openstack	Cloud Magnum Orchestration	7	All	All	All
Application	Openstack	Cloud Magnum Orchestration	7	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All

Operating System	Redhat	Enterprise Linux	5	All	server	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	server	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2	All	All	All

Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Long Life	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Long Life	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Suse	Linux Enterprise For Sap	12	sp1	All	All
Operating System	Suse	Linux Enterprise For Sap	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All

Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server For Raspberry Pi	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server For Raspberry Pi	12	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12.0	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12.0	sp2	All	All

References

Reference
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Priv
Red Hat Customer Portal
Debian -- Security Information -- DSA-3887-1 glibc
CVE-2017-1000366 - Red Hat Customer Portal
McAfee Corporate KB - McAfee Security Bulletin - Web Gateway update fixes vulnerabilities CVE-2012-6706, CVE-2017-1000364, CVE-2017
SUSE products and a new security bug class referred to as "Stack Clash". | Support | SUSE
Full Disclosure: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X
Red Hat Customer Portal
GNU glibc CVE-2017-1000366 Local Memory Corruption Vulnerability
Cisco Device Hardcoded Credentials / GNU glibc / BusyBox ≈ Packet Storm
Bugtraq: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X
Glibc Stack/Heap Memory Allocation Error Lets Local Users Gain Elevated Privileges - SecurityTracker
CVE-2017-1000366 | SUSE
Red Hat Customer Portal
Red Hat Customer Portal
Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/25 / CentOS 5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Clash' Local Privilege Escalation - L
GNU C Library: Multiple vulnerabilities (GLSA 201706-19) — Gentoo security
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash' Local Privilege Escalation - Linux_
www.qualys.com/2017/06/19/stack-clash/stack-clash.txt

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378113 Virtuozzo Linux Security Update for glibc-devel (VZLSA-2017:1481)
- 378114 Virtuozzo Linux Security Update for glibc-devel (VZLSA-2017:1480)
- 378173 Virtuozzo Linux Security Update for glibc-static (VZLSA-2017:1481)
- 6000511 Debian Security Update for glibc (CVE-2017-1000409,CVE-2017-1000366)
- 6000512 Debian Security Update for glibc (CVE-2017-1000408)