



CVE-2018-1000001

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

Summary

CVE	CVE-2018-1000001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-31 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the dest

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Application	Gnu	Glibc	All	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 Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	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
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source	Link
oss-sec: Libc Realpath Buffer Underflow CVE-2018-1000001	MLIST	seclists.org
Libc Realpath Buffer Underflow	MISC	www.halfdog.net
glibc - 'realpath()' Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
February 2018 GNU C Library Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Red Hat Customer Portal	REDHAT	access.redhat.com
GNU glibc CVE-2018-1000001 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
Glibc Buffer Underflow in __realpath() Lets Local Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com
USN-3536-1: GNU C Library vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3534-1: GNU C Library vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
glibc - 'getcwd()' Local Privilege Escalation	EXPLOIT-DB	www.exploit-db.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report