



# CVE-2016-9401

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

## Summary

<b>CVE</b>	CVE-2016-9401
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-01-23 21:59:00 UTC
<b>Updated</b>	2020-09-14 18:32:00 UTC
<b>Description</b>	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch1	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch2	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch3	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch4	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch5	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch1	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch2	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch3	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch4	All	All
Application	<a href="#">Gnu</a>	<a href="#">Bash</a>	4.4	patch5	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	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	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	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	7.7	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	7.7	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	7.7	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	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	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

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
oss-security - Re: bash - popd controlled free	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third Party Advisor
[SECURITY] [DLA 1726-1] bash security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party Advisor
oss-security - bash - popd controlled free	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Third Party Advisor
Red Hat Customer Portal	REDHAT	<a href="https://rhn.redhat.com">rhn.redhat.com</a>	Third Party Advisory
Bash: Multiple vulnerabilities (GLSA 201701-02) — Gentoo Security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory

GNU Bash CVE-2016-9401 Local Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710387](#) Gentoo Linux Bash Multiple Vulnerabilities (GLSA 201701-02)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)