CVE-2016-9401

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-9401
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2020-09-14 18:32:00 UTC
Description	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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Gnu	Bash	All	All	All	All
Application	Gnu	Bash	4.4	patch1	All	All
Application	Gnu	Bash	4.4	patch2	All	All
Application	Gnu	Bash	4.4	patch3	All	All
Application	Gnu	Bash	4.4	patch4	All	All
Application	Gnu	Bash	4.4	patch5	All	All
Application	Gnu	Bash	All	All	All	All
Application	Gnu	Bash	4.4	patch1	All	All
Application	Gnu	Bash	4.4	patch2	All	All
Application	Gnu	Bash	4.4	patch3	All	All
Application	Gnu	Bash	4.4	patch4	All	All
Application	Gnu	Bash	4.4	patch5	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	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	access.redhat.com	Third Party Advisory
oss-security - Re: bash - popd controlled free	MLIST	www.openwall.com	Mailing List, Third Party Advisor
[SECURITY] [DLA 1726-1] bash security update	MLIST	lists.debian.org	Mailing List, Third Party Advisor
oss-security - bash - popd controlled free	MLIST	www.openwall.com	Mailing List, Third Party Advisor
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Advisory
Bash: Multiple vulnerabilities (GLSA 201701-02) — Gentoo Security	GENTOO	security.gentoo.org	Third Party Advisory

GNU Bash CVE-2016-9401 Local Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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