CVE-2018-1071

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1071
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-09 15:29:00 UTC
Updated	2023-02-12 23:32:00 UTC
Description	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the exec.c:hashcmd() function. A local attacker c

Risk And Classification

Problem Types: CWE-121

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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
Application	Zsh	Zsh	All	All	All	All

References

Reference	Source	Link
1553531 – (CVE-2018-1071) CVE-2018-1071 zsh: Stack-based buffer overflow in exec.c:hashcmd()	CONFIRM	bugzilla.redhat.com
[SECURITY] [DLA 2470-1] zsh security update	MLIST	lists.debian.org
Zsh: Multiple vulnerabilities (GLSA 201805-10) — Gentoo security	GENTOO	security.gentoo.org
CVE-2018-1071 - Red Hat Customer Portal	MISC	access.redhat.com
Zsh 'exec.c:hashcmd()' Function Local Denial of Service Vulnerability	BID	www.securityfocus.com
[SECURITY] [DLA 1335-1] zsh security update	MLIST	lists.debian.org
USN-3608-1: Zsh vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.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.

Legacy QID Mappings

- 500832 Alpine Linux Security Update for zsh
- 504569 Alpine Linux Security Update for zsh
- 710220 Gentoo Linux Zsh Multiple Vulnerabilities (GLSA 201805-10)
- 753235 SUSE Enterprise Linux Security Update for zsh (SUSE-SU-2022:14910-1)