



# CVE-2018-1071

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

## Summary

<b>CVE</b>	CVE-2018-1071
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-03-09 15:29:00 UTC
<b>Updated</b>	2023-02-12 23:32:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	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>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Zsh</a>	<a href="#">Zsh</a>	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	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
[SECURITY] [DLA 2470-1] zsh security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Zsh: Multiple vulnerabilities (GLSA 201805-10) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
CVE-2018-1071 - Red Hat Customer Portal	MISC	<a href="https://access.redhat.com">access.redhat.com</a>
Zsh 'exec.c:hashcmd()' Function Local Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] [DLA 1335-1] zsh security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
USN-3608-1: Zsh vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)

© [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](https://status.cve.report)