



CVE-2019-20044

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

Summary

CVE	CVE-2019-20044
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-24 14:15:00 UTC
Updated	2023-11-07 03:08:00 UTC
Description	In Zsh before 5.8, attackers able to execute commands can regain privileges dropped by the --no-PRIVILEGED option. Zsh

Risk And Classification

Problem Types: CWE-273

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.13.6	-	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2018-002	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2018-003	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-001	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-002	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-003	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2019-007	All	All

Operating System	Apple	Mac Os X	10.13.6	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.13.6	security_update_2020-002	All	All
Operating System	Apple	Mac Os X	10.14.6	-	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-001	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-002	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-007	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-002	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Zsh	Zsh	All	All	All	All
Application	Zsh	Zsh	All	All	All	All

References

Reference

About the security content of macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra - Apple Support

[SECURITY] Fedora 30 Update: zsh-5.7.1-6.fc30 - package-announce - Fedora Mailing-Lists

About the security content of watchOS 6.2.5 - Apple Support

ZSH - Release Notes

Full Disclosure: APPLE-SA-2020-05-26-5 watchOS 6.2.5

About the security content of tvOS 13.4.5 - Apple Support

About the security content of tvOS 13.4.5 - Apple Support

GitHub - XMB5/zsh-privileged-upgrade: ZSH Exploit allowing a user to restore privileges dropped from --no-PRIVILEGED option

[SECURITY] [DLA 2470-1] zsh security update

Full Disclosure: APPLE-SA-2020-05-26-1 iOS 13.5 and iPadOS 13.5

Zsh: Privilege escalation (GLSA 202003-55) — Gentoo security

Apple Support Communities: macOS 10.15.5, Security Update 2020-003

About the security content of watchOS 6.2.5 - Apple Support

About the security content of macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra - Apple Support

www.zsh.org/mla/zsh-announce/141

About the security content of iOS 13.5 and iPadOS 13.5 - Apple Support

[SECURITY] Fedora 30 Update: zsh-5.7.1-6.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2117-1] zsh security update

About the security content of iOS 13.5 and iPadOS 13.5 - Apple Support

[SECURITY] Fedora 31 Update: zsh-5.7.1-6.fc31 - package-announce - Fedora Mailing-Lists

Full Disclosure: APPLE-SA-2020-05-26-4 tvOS 13.4.5

[SECURITY] Fedora 31 Update: zsh-5.7.1-6.fc31 - package-announce - Fedora Mailing-Lists

Full Disclosure: APPLE-SA-2020-05-26-3 macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198699](#) Ubuntu Security Notification for Zsh Vulnerabilities (USN-5325-1)

[296073](#) Oracle Solaris 11.4 Support Repository Update (SRU) 24.75.2 Missing (CPUJUL2020)

[376894](#) Alibaba Cloud Linux Security Update for zsh (ALINUX3-SA-2022:0073)

[377075](#) Alibaba Cloud Linux Security Update for zsh (ALINUX2-SA-2020:0031)

[500833](#) Alpine Linux Security Update for zsh

[504570](#) Alpine Linux Security Update for zsh

[751797](#) SUSE Enterprise Linux Security Update for zsh (SUSE-SU-2022:0732-1)

[751799](#) SUSE Enterprise Linux Security Update for zsh (SUSE-SU-2022:0733-1)

[751806](#) SUSE Enterprise Linux Security Update for zsh (SUSE-SU-2022:0735-1)

[751807](#) OpenSUSE Security Update for zsh (openSUSE-SU-2022:0735-1)

[753235](#) SUSE Enterprise Linux Security Update for zsh (SUSE-SU-2022:14910-1)

[940252](#) AlmaLinux Security Update for zsh (ALSA-2020:0903)

[960812](#) Rocky Linux Security Update for zsh (RLSA-2020:0903)

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](#)