



CVE-2021-3156

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

Summary

CVE	CVE-2021-3156
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 21:15:00 UTC
Updated	2024-02-04 09:15:00 UTC
Description	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege esc

Risk And Classification

EPSS: 0.924830000 probability, percentile 0.997300000 (date 2026-04-01)

CISA KEV: Listed on 2022-04-06; due 2022-04-27; ransomware use Unknown

Problem Types: CWE-193

CISA Known Exploited Vulnerability

Vendor	Sudo
Product	Sudo
Name	Sudo Heap-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-3156

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Beyondtrust	Privilege Management For Mac	All	All	All	All
Application	Beyondtrust	Privilege Management For Mac	All	All	All	All
Application	Beyondtrust	Privilege Management For Unix/linux	All	All	All	All
Application	Beyondtrust	Privilege Management For Unix/linux	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Operating System	Fedora	Fedora	32	All	All	All
Operating System	Fedora	Fedora	33	All	All	All
Operating System	Fedora	Fedora	32	All	All	All
Operating System	Fedora	Fedora	33	All	All	All
Application	Mcafee	Web Gateway	10.0.4	All	All	All
Application	Mcafee	Web Gateway	8.2.17	All	All	All
Application	Mcafee	Web Gateway	9.2.8	All	All	All
Application	Mcafee	Web Gateway	10.0.4	All	All	All
Application	Mcafee	Web Gateway	8.2.17	All	All	All
Application	Mcafee	Web Gateway	9.2.8	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Oncommand Unified Manager Core Package	-	All	All	All
Application	Netapp	Oncommand Unified Manager Core Package	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Oracle	Communications Performance Intelligence Center	All	All	All	All
Application	Oracle	Communications Performance Intelligence Center	All	All	All	All
Hardware	Oracle	Micros Compact Workstation 3	-	All	All	All
Operating System	Oracle	Micros Compact Workstation 3 Firmware	310	All	All	All
Hardware	Oracle	Micros Es400	-	All	All	All
Operating System	Oracle	Micros Es400 Firmware	All	All	All	All
Hardware	Oracle	Micros Kitchen Display System	-	All	All	All
Operating System	Oracle	Micros Kitchen Display System Firmware	210	All	All	All
Hardware	Oracle	Micros Workstation 5a	-	All	All	All
Operating System	Oracle	Micros Workstation 5a Firmware	5a	All	All	All
Hardware	Oracle	Micros Workstation 6	-	All	All	All
Operating System	Oracle	Micros Workstation 6 Firmware	All	All	All	All
Application	Oracle	Tekelec Platform Distribution	All	All	All	All
Application	Sudo Project	Sudo	All	All	All	All
Application	Sudo Project	Sudo	1.9.5	-	All	All
Application	Sudo Project	Sudo	1.9.5	patch1	All	All
Application	Sudo Project	Sudo	All	All	All	All
Application	Sudo Project	Sudo	1.9.5	patch1	All	All
Application	Synology	Diskstation Manager	6.2	All	All	All

Application	Synology	Diskstation Manager	6.2	All	All	All
Application	Synology	Diskstation Manager Unified Controller	3.0	All	All	All
Application	Synology	Diskstation Manager Unified Controller	3.0	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Hardware	Synology	Skynas	-	All	All	All
Operating System	Synology	Skynas Firmware	-	All	All	All
Operating System	Synology	Skynas Firmware	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All

References

Reference

oss-security - Re: Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)

oss-security - Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)

CVE-2021-3156 Sudo Vulnerability in NetApp Products | NetApp Product Security

oss-security - Re: CVE-2023-6246: Heap-based buffer overflow in the glibc's syslog()

Full Disclosure: Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)

glibc syslog() Heap-Based Buffer Overflow ≈ Packet Storm

Sudo Stable Release

Sudo Buffer Overflow / Privilege Escalation ≈ Packet Storm

[SECURITY] Fedora 32 Update: sudo-1.9.5p2-1.fc32 - package-announce - Fedora Mailing-Lists

Oracle Critical Patch Update Advisory - April 2022

[SECURITY] [DLA 2534-1] sudo security update

oss-security - CVE-2023-6246: Heap-based buffer overflow in the glibc's syslog()

[SECURITY] Fedora 33 Update: sudo-1.9.5p2-1.fc33 - package-announce - Fedora Mailing-Lists

Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021

oss-security - Re: Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)

Oracle Critical Patch Update Advisory - July 2021

CVE-2020-8585 Sensitive Information Disclosure Vulnerability in OnCommand Unified Manager Core Package | NetApp Product Security

Oracle Critical Patch Update Advisory - October 2021

Debian -- Security Information -- DSA-4839-1 sudo

Sudo Heap-Based Buffer Overflow ≈ Packet Storm

oss-security - Re: sudo: Ineffective NO_ROOT_MAILER and Baron Samedit

[SECURITY] Fedora 32 Update: sudo-1.9.5p2-1.fc32 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 33 Update: sudo-1.9.5p2-1.fc33 - package-announce - Fedora Mailing-Lists

Full Disclosure: CVE-2023-6246: Heap-based buffer overflow in the glibc's syslog()

VU#794544 - Heap-Based Buffer Overflow in Sudo

Sudo 1.8.31p2 / 1.9.5p1 Buffer Overflow ≈ Packet Storm

oss-security - Baron Samedit: Heap-based buffer overflow in Sudo (CVE-2021-3156)

Sudo 1.9.5p1 Buffer Overflow / Privilege Escalation ≈ Packet Storm

oss-security - Re: Oracle Solaris membership in the distros list

McAfee Security Bulletin - Status and updates for Linux sudo vulnerability (CVE-2021-3156)

sudo: Multiple vulnerabilities (GLSA 202101-33) — Gentoo security

Security Advisory: Privilege Management for Unix & Linux Basic & Privilege Management for Mac | BeyondTrust

Full Disclosure: APPLE-SA-2021-02-09-1 macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, and macOS Mojave 10.14.6 Security Update

About the security content of macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, and macOS Mojave 10.14.6 Security Update

Synology Inc.

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159156](#) Oracle Enterprise Linux Security Update for sudo (ELSA-2021-9169)

[174831](#) SUSE Enterprise Linux Security update for sudo (SUSE-SU-2021:0928-1)

[174850](#) SUSE Enterprise Linux Security update for sudo (SUSE-SU-2021:0928-1)

[174930](#) SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2021:1275-1)

[174931](#) SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2021:1274-1)

[174932](#) SUSE Enterprise Linux Security Update for sudo (SUSE-SU-2021:1273-1)

[180137](#) Debian Security Update for sudo (CVE-2021-3156)

[375648](#) Centrify Service Suite agent (DirectControl) Privilege Escalation Vulnerability

[376875](#) Alibaba Cloud Linux Security Update for sudo (ALINUX2-SA-2021:0003)

[377324](#) Alibaba Cloud Linux Security Update for sudo (ALINUX3-SA-2022:0113)

[380227](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for sudo (OVMSA-2021-0012)

390227 Oracle managed virtualization (VM) Server for x86 Security Update for sudo (OVMSA-2021-0012)
390235 Oracle Managed Virtualization (VM) Server for x86 Security Update for sudo (OVMSA-2021-0003)
43855 HPE ArubaOS Sudo Privilege Escalation Vulnerability (ARUBA-PSA-2021-015)
500678 Alpine Linux Security Update for sudo
506250 Alpine Linux Security Update for sudo
670208 EulerOS Security Update for sudo (EulerOS-SA-2021-1707)
690352 Free Berkeley Software Distribution (FreeBSD) Security Update for sudo (f3cf4b33-6013-11eb-9a0e-206a8a720317)
730227 McAfee Web Gateway Multiple Vulnerabilities (WP-3426, WP-3427, WP-3307, WP-3444, WP-3452, WP-3475)
750253 OpenSUSE Security Update for sudo (openSUSE-SU-2021:0602-1)
940237 AlmaLinux Security Update for sudo (ALSA-2021:0218)

© [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](#)