



CVE-2021-45417

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-45417 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-01-20 18:15:00 UTC |
| Updated | 2023-11-25 09:15:00 UTC |
| Description | AIDE before 0.17.4 allows local users to obtain root privileges via crafted file metadata (such as XFS extended attributes or |

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | E |
|------------------|--|--|---------|--------|---|
| Application | Advanced Intrusion Detection Environment Project | Advanced Intrusion Detection Environment | All | All | A |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | A |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | A |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | A |
| Operating System | Canonical | Ubuntu Linux | 20.04 | All | A |
| Operating System | Canonical | Ubuntu Linux | 21.04 | All | A |
| Operating System | Canonical | Ubuntu Linux | 21.10 | All | A |
| Operating System | Debian | Debian Linux | 10.0 | All | A |
| Operating System | Debian | Debian Linux | 11.0 | All | A |
| Operating System | Debian | Debian Linux | 9.0 | All | A |
| Operating System | Fedoraproject | Fedora | 35 | All | A |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | A |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | A |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | A |
| Application | Redhat | Ovirt-node | 4.4.10 | All | A |
| Application | Redhat | Virtualization Host | 4.0 | All | A |

References

| Reference | Source | Link |
|--|---------|--------------------------|
| Debian -- Security Information -- DSA-5051-1 aide | DEBIAN | www.d |
| oss-security - CVE-2021-45417 - aide (>= 0.13 <= 0.17.3): heap-based buffer overflow vulnerability in base64 functions | MISC | www.o |
| [Aide] CVE-2021-45417 - aide (>= 0.13 <= 0.17.3): heap-based buffer overflow vulnerability in base64 functions | MISC | www.iq |
| [SECURITY] [DLA 2894-1] aide security update | MLIST | lists.de |
| AIDE: Root Privilege Escalation (GLSA 202311-07) — Gentoo security | | securit |
| oss-security - CVE-2021-45417 - aide (>= 0.13 <= 0.17.3): heap-based buffer overflow vulnerability in base64 functions | MLIST | www.o |
| CVE Program record | CVE.ORG | www.c |
| NVD vulnerability detail | NVD | nvd.nis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|--|
| 159627 Oracle Enterprise Linux Security Update for aide (ELSA-2022-0441) |
| 159629 Oracle Enterprise Linux Security Update for aide (ELSA-2022-0473) |
| 159643 Oracle Enterprise Linux Security Update for aide (ELSA-2022-9165) |
| 179011 Debian Security Update for aide (DSA 5051-1) |
| 179026 Debian Security Update for aide (DLA 2894-1) |
| 182488 Debian Security Update for aide (CVE-2021-45417) |
| 198639 Ubuntu Security Notification for AIDE Vulnerability (USN-5243-1) |
| 240065 Red Hat Update for aide (RHSA-2022:0441) |
| 240066 Red Hat Update for aide (RHSA-2022:0440) |
| 240070 Red Hat Update for aide (RHSA-2022:0456) |
| 240071 Red Hat Update for aide (RHSA-2022:0473) |
| 240446 Red Hat Update for aide (RHSA-2022:0464) |
| 257152 CentOS Security Update for aide (CESA-2022:0473) |
| 353950 Amazon Linux Security Advisory for aide : ALAS-2022-1587 |
| 354063 Amazon Linux Security Advisory for aide : ALAS2-2022-1850 |
| 377155 Alibaba Cloud Linux Security Update for aide (ALINUX3-SA-2022:0009) |
| 377197 Alibaba Cloud Linux Security Update for aide (ALINUX2-SA-2022:0011) |

| |
|--|
| 671443 EulerOS Security Update for aide (EulerOS-SA-2022-1421) |
| 671466 EulerOS Security Update for aide (EulerOS-SA-2022-1442) |
| 671593 EulerOS Security Update for aide (EulerOS-SA-2022-1556) |
| 671619 EulerOS Security Update for aide (EulerOS-SA-2022-1656) |
| 671629 EulerOS Security Update for aide (EulerOS-SA-2022-1642) |
| 671682 EulerOS Security Update for aide (EulerOS-SA-2022-1702) |
| 690777 Free Berkeley Software Distribution (FreeBSD) Security Update for aide (309c35f4-7c9f-11ec-a739-206a8a720317) |
| 710795 Gentoo Linux AIDE Root Privilege Escalation Vulnerability (GLSA 202311-07) |
| 751627 SUSE Enterprise Linux Security Update for aide (SUSE-SU-2022:0145-1) |
| 751634 SUSE Enterprise Linux Security Update for aide (SUSE-SU-2022:0150-1) |
| 751636 OpenSUSE Security Update for aide (openSUSE-SU-2022:0150-1) |
| 751751 OpenSUSE Security Update for aide (openSUSE-SU-2022:0150-2) |
| 753126 SUSE Enterprise Linux Security Update for aide (SUSE-SU-2022:14879-1) |
| 940450 AlmaLinux Security Update for aide (ALSA-2022:0441) |
| 960110 Rocky Linux Security Update for aide (RLSA-2022:441) |
| 960757 Rocky Linux Security Update for aide (RLSA-2022:0441) |

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)