



CVE-2022-43634

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

Summary

CVE	CVE-2022-43634
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 19:15:00 UTC
Updated	2023-11-07 03:54:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required for this exploit. An attacker could use this vulnerability to execute arbitrary code on the remote host. This vulnerability is due to a buffer overflow in the Netatalk daemon. A remote attacker could exploit this vulnerability to execute arbitrary code on the remote host. Authentication is not required for this exploit. An attacker could use this vulnerability to execute arbitrary code on the remote host. This vulnerability is due to a buffer overflow in the Netatalk daemon. A remote attacker could exploit this vulnerability to execute arbitrary code on the remote host. Authentication is not required for this exploit. An attacker could use this vulnerability to execute arbitrary code on the remote host.

Risk And Classification

Problem Types: CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netatalk	Netatalk	3.1.13	All	All	All
Application	Netatalk Project	Netatalk	3.1.13	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 36 Update: netatalk-3.1.14-3.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 38 Update: netatalk-3.1.14-3.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
fix CVE-2022-43634 by eh-syn · Pull Request #186 · Netatalk/Netatalk · GitHub	MISC	github.com
[SECURITY] Fedora 37 Update: netatalk-3.1.14-3.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: netatalk-3.1.14-3.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 38 Update: netatalk-3.1.14-3.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-5503-1 netatalk	DEBIAN	www.debian.org
[SECURITY] [DLA 3426-1] netatalk security update	MLIST	lists.debian.org
[SECURITY] Fedora 36 Update: netatalk-3.1.14-3.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
ZDI-23-094 Zero Day Initiative	MISC	www.zerodayinitiative.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

181789	Debian Security Update for netatalk (DLA 3426-1)
199403	Ubuntu Security Notification for Netatalk Vulnerabilities (USN-6146-1)
283871	Fedora Security Update for netatalk (FEDORA-2023-e714897e70)
283872	Fedora Security Update for netatalk (FEDORA-2023-aaeb45fb73)
284201	Fedora Security Update for netatalk (FEDORA-2023-599faf1b1c)
502991	Alpine Linux Security Update for netatalk
505769	Alpine Linux Security Update for netatalk
6000181	Debian Security Update for netatalk (DSA 5503-1)
753650	SUSE Enterprise Linux Security Update for netatalk (SUSE-SU-2023:0316-1)

© 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](#)