



CVE-2022-23122

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

Summary

CVE	CVE-2022-23122
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-28 19:15:00 UTC
Updated	2023-11-22 21:03:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required for this exploit. The vulnerability is due to a buffer overflow in the Netatalk daemon. An attacker can exploit this by sending a specially crafted request to the Netatalk daemon. This results in the execution of arbitrary code on the system. The vulnerability affects Netatalk versions 3.11.0 and earlier.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Netatalk	Netatalk	All	All	All	All
Application	Netatalk Project	Netatalk	All	All	All	All

References

Reference	Source	Link
Netatalk: Multiple Vulnerabilities including root remote code execution (GLSA 202311-02) — Gentoo security	GENTOO	security.gentoo.org
Netatalk Release Notes	MISC	netatalk.sourceforge.net
ZDI-22-529 Zero Day Initiative	MISC	www.zerodayinitiative.com
Debian -- Security Information -- DSA-5503-1 netatalk	DEBIAN	www.debian.org
[SECURITY] [DLA 3426-1] netatalk security update	MLIST	lists.debian.org
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)

502549 Alpine Linux Security Update for netatalk

505087 Alpine Linux Security Update for netatalk

6000181 Debian Security Update for netatalk (DSA 5503-1)

710785 Gentoo Linux Netatalk Multiple Vulnerabilities including root Remote Code Execution (RCE) (GLSA 202311-02)

© [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](#)