



# CVE-2022-23125

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

## Summary

<b>CVE</b>	CVE-2022-23125
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-28 19:15:00 UTC
<b>Updated</b>	2023-12-28 15:12:00 UTC
<b>Description</b>	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required for this vulnerability to be exploited. The attack requires successful remote authentication to the affected system and user interaction via a remote user. The vulnerability is due to a buffer overflow in the Netatalk daemon. A remote attacker can exploit this vulnerability to execute arbitrary code on the target system. Authentication is not required for this vulnerability to be exploited. The attack requires successful remote authentication to the affected system and user interaction via a remote user. The vulnerability is due to a buffer overflow in the Netatalk daemon. A remote attacker can exploit this vulnerability to execute arbitrary code on the target system.

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Netatalk</a>	<a href="#">Netatalk</a>	All	All	All	All
Application	<a href="#">Netatalk Project</a>	<a href="#">Netatalk</a>	All	All	All	All

## References

Reference	Source	Link
Netatalk: Multiple Vulnerabilities including root remote code execution (GLSA 202311-02) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.o</a>
ZDI-22-526   Zero Day Initiative	MISC	<a href="https://www.zerodayinitiative.com">www.zerodayiniti</a>
Netatalk Release Notes	MISC	<a href="https://netatalk.sourceforge.net">netatalk.sourcefo</a>
Debian -- Security Information -- DSA-5503-1 netatalk	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 3426-1] netatalk security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)

[752037](#) SUSE Enterprise Linux Security Update for netatalk (SUSE-SU-2022:1184-1)

© [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](#)