CVE-2022-23125

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-23125
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	2023-12-28 15:12:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is nc

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.o
ZDI-22-526 | Zero Day Initiative	MISC	www.zerodayiniti
Netatalk Release Notes	MISC	netatalk.sourcefo
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)

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