



# CVE-2022-45188

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

## Summary

<b>CVE</b>	CVE-2022-45188
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-12 05:15:00 UTC
<b>Updated</b>	2023-12-28 15:12:00 UTC
<b>Description</b>	Netatalk through 3.1.13 has an afp_getappl heap-based buffer overflow resulting in code execution via a crafted .appl file. T

## 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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	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
[SECURITY] Fedora 36 Update: netatalk-3.1.14-3.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 38 Update: netatalk-3.1.14-3.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
netatalk - Browse /netatalk at SourceForge.net	MISC	<a href="#">sourceforge.net</a>
Netatalk: Multiple Vulnerabilities including root remote code execution (GLSA 202311-02) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 37 Update: netatalk-3.1.14-3.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 37 Update: netatalk-3.1.14-3.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[1day to 0day] Netatalk from Pwn2own 2021 to 0x00 cent in 2022 - Bla Bla blog	MISC	<a href="#">rushbnt.github.io</a>

[SECURITY] Fedora 38 Update: netatalk-3.1.14-3.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Netatalk Release Notes	MISC	<a href="https://netatalk.sourceforge.net">netatalk.sourceforge.net</a>
Debian -- Security Information -- DSA-5503-1 netatalk	DEBIAN	<a href="http://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>
[SECURITY] Fedora 36 Update: netatalk-3.1.14-3.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Encountered a 404 error	MISC	<a href="https://netatalk.sourceforge.net">netatalk.sourceforge.net</a>
CVE Program record	CVE.ORG	<a href="http://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

<a href="#">181789</a> Debian Security Update for netatalk (DLA 3426-1)
<a href="#">199403</a> Ubuntu Security Notification for Netatalk Vulnerabilities (USN-6146-1)
<a href="#">283871</a> Fedora Security Update for netatalk (FEDORA-2023-e714897e70)
<a href="#">283872</a> Fedora Security Update for netatalk (FEDORA-2023-aaeb45fb73)
<a href="#">284201</a> Fedora Security Update for netatalk (FEDORA-2023-599faf1b1c)
<a href="#">502991</a> Alpine Linux Security Update for netatalk
<a href="#">505769</a> Alpine Linux Security Update for netatalk
<a href="#">6000181</a> Debian Security Update for netatalk (DSA 5503-1)
<a href="#">710785</a> Gentoo Linux Netatalk Multiple Vulnerabilities including root Remote Code Execution (RCE) (GLSA 202311-02)
<a href="#">752998</a> SUSE Enterprise Linux Security Update for netatalk (SUSE-SU-2022:4360-1)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**