



# CVE-2022-22995

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

## Summary

<b>CVE</b>	CVE-2022-22995
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@wdc.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-25 23:15:00 UTC
<b>Updated</b>	2024-01-04 22:15:00 UTC
<b>Description</b>	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By e

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	39	All	All	All
Application	<a href="#">Netatalk</a>	<a href="#">Netatalk</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud</a>	-	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud DI2100</a>	-	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud DI2100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud DI4100</a>	-	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud DI4100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex2100</a>	-	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex2100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex2 Ultra</a>	-	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex2 Ultra Firmware</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex4100</a>	-	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud Ex4100 Firmware</a>	All	All	All	All
Operating System	<a href="#">Westerndigital</a>	<a href="#">My Cloud Firmware</a>	All	All	All	All
Hardware	<a href="#">Westerndigital</a>	<a href="#">My Cloud Home</a>	-	All	All	All

Operating System	Westerndigital	My Cloud Home Firmware	All	All	All	All
Hardware	Westerndigital	My Cloud Mirror Gen 2	-	All	All	All
Operating System	Westerndigital	My Cloud Mirror Gen 2 Firmware	All	All	All	All
Hardware	Westerndigital	My Cloud Pr2100	-	All	All	All
Operating System	Westerndigital	My Cloud Pr2100 Firmware	All	All	All	All
Hardware	Westerndigital	My Cloud Pr4100	-	All	All	All
Operating System	Westerndigital	My Cloud Pr4100 Firmware	All	All	All	All
Hardware	Westerndigital	Wd Cloud	-	All	All	All
Operating System	Westerndigital	Wd Cloud Firmware	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 38 Update: netatalk-3.1.18-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</a>
[SECURITY] Fedora 38 Update: netatalk-3.1.18-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</a>
WDC-22005 Netatalk Security Vulnerabilities   Western Digital	MISC	<a href="http://www.westerndigital.com/">www.westerndigital.com/</a>
[SECURITY] Fedora 37 Update: netatalk-3.1.18-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</a>
Netatalk: Multiple Vulnerabilities including root remote code execution (GLSA 202311-02) — Gentoo security	GENTOO	<a href="https://security.gentoo.org/">security.gentoo.org/</a>
[SECURITY] Fedora 37 Update: netatalk-3.1.18-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</a>
[debian-lts-announce] 20240104 [SECURITY] [DLA 3706-1] netatalk security update		<a href="https://lists.debian.org/">lists.debian.org/</a>
[SECURITY] Fedora 39 Update: netatalk-3.1.18-1.fc39 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</a>
[SECURITY] Fedora 39 Update: netatalk-3.1.18-1.fc39 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org/</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>

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Corentin BAYET (@OnlyTheDuck), Etienne HELLUY-LAFONT and Luca MORO (@johncool\_\_) from Synacktiv working with Trend Micro's Zero Day Initiative

## Legacy QID Mappings

[284623](#) Fedora Security Update for netatalk (FEDORA-2023-ef901c862c)

[284624](#) Fedora Security Update for netatalk (FEDORA-2023-cec97f7b5d)

[285217](#) Fedora Security Update for netatalk (FEDORA-2023-39f0ec3879)

[503372](#) Alpine Linux Security Update for netatalk

506123 Alpine Linux Security Update for netatalk

6000420 Debian Security Update for netatalk (DLA 3706-1)

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

755094 SUSE Enterprise Linux Security Update for netatalk (SUSE-SU-2023:4084-1)

© [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](#)