



CVE-2021-32708

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-32708
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-24 17:15:00 UTC
Updated	2023-11-07 03:35:00 UTC
Description	Flysystem is an open source file storage library for PHP. The whitespace normalisation using in 1.x and 2.x removes any ur

Risk And Classification

Problem Types: CWE-367

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Thephpleague	Flysystem	All	All	All	All

References

Reference	Source	Link
Reject paths with funky whitespace. · thephpleague/flysystem@f3ad691 · GitHub	MISC	github
[SECURITY] Fedora 34 Update: php-league-flysystem-1.1.4-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fe
league/flysystem - Packagist	MISC	packa
[SECURITY] Fedora 33 Update: php-league-flysystem-1.1.4-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fe
Time-of-check Time-of-use (TOCTOU) Race Condition in league/flysystem · Advisory · thephpleague/flysystem · GitHub	CONFIRM	github
[SECURITY] Fedora 34 Update: php-league-flysystem-1.1.4-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fe
Reject funky whitespace paths. · thephpleague/flysystem@a3c694d · GitHub	MISC	github
[SECURITY] Fedora 33 Update: php-league-flysystem-1.1.4-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fe
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180011](#) Debian Security Update for php-league-flysystem (CVE-2021-32708)

[281680](#) Fedora Security Update for php (FEDORA-2021-717516a2e9)

[281681](#) Fedora Security Update for php (FEDORA-2021-b9187c535c)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)