



# Simple File List <= 3.2.7 - Arbitrary File Download

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

## Summary

<b>CVE</b>	CVE-2022-1119
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-19 21:15:13 UTC
<b>Updated</b>	2026-04-08 19:17:49 UTC
<b>Description</b>	The Simple File List WordPress plugin is vulnerable to Arbitrary File Download via the eeFile parameter found in the ~/inclu

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**EPSS:** 0.857720000 probability, percentile 0.993790000 (date 2026-04-08)

**Problem Types:** CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	security@wordfence.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Simplefilelist</a>	<a href="#">Simple-file-list</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Eemitch</a>	<a href="#">Simple File List</a>	affected 3.2.7 semver	Not specified

### References

Reference	Source	Link	Tags
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	<a href="#">plugins.trac.wordpress.org</a>	Patch, Third Party
Attention Required!   Cloudflare	af854a3a-2127-422b-91ae-364da2661108	<a href="#">wpscan.com</a>	Exploit, Third Party
Simple File List <= 3.2.7 - Arbitrary File Download	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.wordfence.com</a>	
Arbitrary File Download - Google Docs	af854a3a-2127-422b-91ae-364da2661108	<a href="#">docs.google.com</a>	Exploit, Third Party
Vulnerability Advisories - Wordfence	MITRE	<a href="#">www.wordfence.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical

## Vendor Comments And Credit

## Discovery Credit

**CNA:** Bernardo Rodrigues (en)**CNA:** Admavidhya N (en)

## Additional Advisory Data

Source	Time	Event
CNA	2019-05-23T00:00:00.000Z	Disclosed

There are currently no legacy QID mappings associated with this CVE.

© [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](#)