HTTP Headers <= 1.19.2 - Authenticated (Administrator+) External Control of File Name or Path to RCE via 'hh_htpasswd_path' and 'hh_www_authenticate_user' Parameters

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4132
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 09:16:24 UTC
Updated	2026-04-22 09:16:24 UTC
Description	The HTTP Headers plugin for WordPress is vulnerable to External Control of File Name or Path leading to Remote Code Ex

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from security@wordfence.com

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

Problem Types: CWE-73 | CWE-73 CWE-73 External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zinoui	HTTP Headers	affected 1.19.2 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/ce010c6f-16bd-4178-a621-31ba6...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/tags/1.19.2/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/http-headers/trunk/http-headers.php	security@wordfence.com	plugins.trac.wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Chiao-Lin Yu (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-21T19:13:19.000Z	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 registred 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**