



WordPress WP Pipes plugin <= 1.4.2 - Arbitrary File Deletion Vulnerability

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

Summary

CVE	CVE-2025-48267
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-09 16:15:44 UTC
Updated	2026-04-28 19:32:41 UTC
Description	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThimPress WP Pipes allows P

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from nvd@nist.gov

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

EPSS: 0.003750000 probability, percentile 0.591360000 (date 2026-04-28)

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	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	audit@patchstack.com	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/N/I:N/A:H
3.1	CNA	CVSS	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thimpress	Wp Pipes	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ThimPress	WP Pipes	affected n/a 1.4.2 custom	Not specified

References

Reference

[patchstack.com/database/wordpress/plugin/wp-pipes/vulnerability/wordpress-wp...](https://patchstack.com/database/wordpress/plugin/wp-pipes/vulnerability/wordpress-wp-pipes-1-4-2-arbitrary-file-deletion-vulnerability?_s_id=...)

https://patchstack.com/database/wordpress/plugin/wp-pipes/vulnerability/wordpress-wp-pipes-1-4-2-arbitrary-file-deletion-vulnerability?_s_id=...

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: timomangcut (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress WP Pipes plugin to the latest available version (at least 1.4.3).

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

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