INTELLIGENCE

As a reminder, the Wordfence Intelligence Vulnerability Database API is completely free to query and utilize, both personally and commercially, and contains all the same vulnerability data as the user interface. Please review the API documentation and Webhook documentation for more information on how to query the vulnerability API endpoints and configure webhooks utilizing all the same data present in the Wordfence Intelligence user interface.

Envolve Plugin <= 1.0 - Unauthenticated Language File Deletion

5.3

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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

CVE	CVE-2024-11615
CVSS	5.3 (Medium)
Publicly Published	May 5, 2025
Last Updated	May 5, 2025
Researcher	István Márton - Wordfence

Description

The Envolve Plugin plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 1.0 via the 'zetra_deleteLanguageFile' and 'zetra_deleteFontsFile' functions. This is due to the plugin not properly validating a file or its path prior to deleting it. This makes it possible for unauthenticated attackers to delete language files.
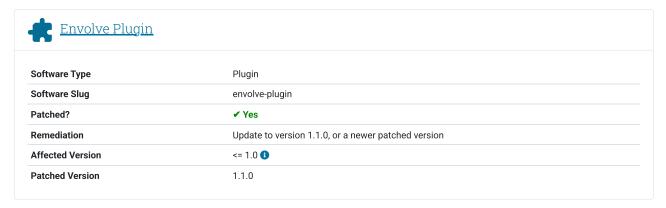
References

- themeforest.net

Share

Facebook   Twitter   LinkedIn   Email

Vulnerability Details for Envolve Plugin

Envolve Plugin

Software Type	Plugin
Software Slug	envolve-plugin
Patched?	✔ Yes
Remediation	Update to version 1.1.0, or a newer patched version
Affected Version	<= 1.0 ⓘ
Patched Version	1.1.0

Have information to add, or spot any errors? Contact us at wfi-support@wordfence.com so we can make any appropriate adjustments.

Did you know Wordfence Intelligence provides free personal and commercial API access to our comprehensive WordPress vulnerability database, along with a free webhook integration to stay on top of the latest vulnerabilities added and updated in the database? Get started today!

LEARN MORE

Want to get notified of the latest vulnerabilities that may affect your WordPress site?
Install Wordfence on your site today to get notified immediately if your site is affected by a vulnerability that has been added to our database.

GET WORDFENCE

The Wordfence Intelligence WordPress vulnerability database is completely free to access and query via API. Please review the documentation on how to access and consume the vulnerability data via API.

DOCUMENTATION

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service

Privacy Policy and Notice at Collection

Products

Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence CLI
Wordfence Intelligence
Wordfence Central

Support

Documentation
Learning Center
Free Support
Premium Support

News

Blog
In The News
Vulnerability Advisories

About

About Wordfence
Affiliate Program
Careers
Contact
Security
CVE Request Form

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

☐ By checking this box I agree to the terms of service and privacy policy.*

SIGN UP