Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# One Empty File to Full Takeover: Elementor Pro Under Active Attack


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| September 04, 2026 | A1 | TA2026257 |

# Summary

**First Seen:** July 2026
**Affected Products:** Elementor Pro (WordPress plugin), versions 4.2.1 and earlier
**Impact:** A critical flaw in Elementor Pro, one of the most widely deployed WordPress page builders with more than 10+ million active installations, is being exploited in the wild to seize complete control of vulnerable websites. Tracked as CVE-2026-32475, the vulnerability lets an attacker upload an executable PHP file through a plugin feature as ordinary as a contact or job-application form. Once that file is on the server and requested through the browser, it runs as code, handing the attacker a foothold from which they can steal data, deface the site, or plant a persistent payload. Because the flaw sits in the Forms module's File Upload field, any site running a published form that accepts attachments is a candidate target, and that is an extremely common setup. With exploitation already active and attackers deploying web shells to take over sites, updating to the patched release is an urgent priority.

## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-32475 | WordPress Elementor Pro Unauthenticated Arbitrary File Upload Vulnerability | WordPress Elementor Pro | ✗ | ✗ | ✓ |

# Vulnerability Details

**#1**

CVE-2026-32475 is a critical unauthenticated arbitrary file upload vulnerability in the Forms module of Elementor Pro. It affects every version of the plugin up to and including 4.2.1. The weakness lives in the File Upload form field, the everyday feature that lets site visitors attach a document, photo, or resume when they submit a contact, support, or job-application form, and it turns that harmless-looking field into a path for running attacker-supplied code on the server.

**#2**

At the heart of the flaw is a disagreement between two pieces of the plugin's own code. When a form is submitted, one routine checks each uploaded file's extension against a blocklist that bans PHP and other executable types, while a second routine moves the accepted files into a public folder. The two disagree on how to handle an empty upload slot: the checker stops entirely the moment it hits one, whereas the mover only skips it and keeps going. An attacker abuses this by sending two file parts under the same field, an empty one first and a PHP payload second, so the validator quits before ever inspecting the payload while the mover writes it into a web-accessible directory.

**#3**

Exploitation needs no authentication and no user interaction. The request goes to the plugin's public form-submission endpoint with no login cookie or security token, and the only prerequisite is a published Elementor form with a File Upload field, a common configuration rather than an exotic one. The file lands in the public forms directory under a randomized name generated from PHP's time-based uniqid() function; because that name is not returned in the response, the attacker recovers it by brute-forcing the narrow time window using the server's own Date header, or simply reads it from the submission-notification email where one is enabled. Requesting the file then executes it, delivering remote code execution.

**#4**

The vendor released a fix in Elementor Pro 4.2.2 on August 19, 2026, which brings the two routines into agreement and re-checks the extension immediately before the file is moved. Notably, active exploitation began the very same day the patch shipped, as attackers reverse-engineered the fix rather than discovering it beforehand. Wordfence reported blocking well over 190,000 exploitation attempts in the days that followed, with attackers deploying web shells to take over sites. Given the plugin's massive install base, the triviality of the exploit, and the fact that a successful upload persists on disk even after patching, the risk to unpatched sites is critical and ongoing.

# Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2026-32475 | WordPress Elementor Pro (Before 4.2.2) | cpe:2.3:a:elementor:elementor_pro:*:*:*:*:*:*:*:* | CWE-434 |

# Recommendations

**Update Elementor Pro Immediately:** Upgrade every affected site to Elementor Pro 4.2.2 or later without delay. This release closes the validation gap and re-checks the file extension right before the upload is saved, and updating is the single fastest and most reliable way to shut the door on this attack. Treat this as an emergency change given that exploitation is already active.

**Inspect the Uploads Directory for Rogue Files:** Because patching stops new attacks but does not remove files an earlier attack already dropped, review the `wp-content/uploads/elementor/forms/` directory on every affected site. Any file ending in `.php`, or any file type your forms do not legitimately accept, should be treated as a compromise indicator and preserved for investigation before removal.

**Assume Breach and Hunt for Compromise:** If you find suspicious files, or if a site ran a vulnerable version with a public file-upload form, act as though a breach may have occurred. Review your WordPress dashboard for unfamiliar administrator accounts, examine server and access logs for unusual POST requests to the form-submission endpoint, reset credentials for trusted accounts, and look for signs of web shell activity or unexpected outbound connections.

**Back Up Your Site Regularly:** Keep automated, frequent backups stored off the live server so that a compromised site can be restored quickly and cleanly. Reliable backups turn a full-takeover incident from a catastrophe into a recoverable event, and they are essential when the only certain way to clear a web shell is to rebuild from a known-good state.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1190: Exploit Public-Facing Application | |
| Execution | T1059: Command and Scripting Interpreter | |
| Persistence | T1505: Server Software Component | T1505.003: Web Shell |
| Resource Development | T1588: Obtain Capabilities | T1588.006: Vulnerabilities |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 185[.]196[.]220[.]85,<br>103[.]84[.]230[.]85,<br>103[.]90[.]148[.]202,<br>216[.]126[.]225[.]208,<br>167[.]254[.]240[.]75,<br>167[.]254[.]241[.]119,<br>114[.]10[.]17[.]253,<br>114[.]10[.]45[.]151, |
| IPv6 | 2602[:]fa59[:]10[:]7a1[:][:]1,<br>2406[:]ef80[:]2[:]7d19[:][:]1, |

## Patch Link

https://wordpress.org/plugins/elementor/

## References

https://www.wordfence.com/blog/2026/09/attackers-actively-exploiting-critical-vulnerability-in-elementor-pro-plugin/

https://patchstack.com/articles/critical-unauthenticated-file-upload-to-rce-in-elementor-pro-plugin/?_s_id=cve

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

**September 04, 2026 • 09:00 AM**



More at www.hivepro.com