

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Forminator Plugin Flaw Can Delete Your Site's Core Files

Date of Publication

July 3, 2025

Admiralty Code

A1

TA Number

TA2025206

Summary

First Seen: June 20, 2025

Affected Product: WordPress Forminator Forms plugin

Impact: CVE-2025-6463 is a high-severity vulnerability in the Forminator Forms WordPress plugin (< v1.44.3) that allows unauthenticated attackers to delete arbitrary files on the server by exploiting unsafe file path handling. If an admin deletes a form entry linked to a malicious submission, critical files like wp-config.php can be removed, potentially leading to full site compromise. With over 600,000 active installations, all users of the Forminator plugin are strongly urged to update immediately or disable the plugin until they can safely upgrade.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-6463	WordPress Forminator Plugin Unauthenticated Arbitrary File Deletion Vulnerability	WordPress Forminator Forms plugin			

Vulnerability Details

#1

CVE-2025-6463 is a high-severity vulnerability found in the Forminator Forms plugin for WordPress (versions prior to 1.44.3). The issue stems from insufficient validation in the `entry_delete_upload_files` function, which allows unauthenticated users to craft form submissions that include arbitrary file paths. When an administrator deletes the associated form entry, either manually or through automatic cleanup, the specified file is deleted from the server. This behavior opens the door for attackers to remove critical files like `wp-config.php`, potentially leading to full site compromise or remote code execution.

#2

The vulnerability is particularly dangerous because it requires no authentication and can be triggered simply by submitting a form with a manipulated file path. While the final deletion step must be initiated by an admin, this action is often routine and, in some cases, automated, making exploitation highly feasible in real-world environments. Given the plugin's wide adoption, with over 600,000 active installations, the attack surface is significant, and many sites may remain unpatched for extended periods.

#3

The flaw rated with a CVSS score of 8.8 (High) due to the combination of high impact and ease of exploitation. The vulnerability was publicly disclosed in late June 2025, and the plugin's maintainers released a patch (version 1.44.3) shortly thereafter. Site owners using the affected plugin versions are strongly urged to update immediately to avoid the risk of arbitrary file deletion and potential system takeover.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-6463	WordPress Forminator Forms plugin versions prior to 1.44.3	cpe:2.3:a:wpmudev:forminator_forms:*:*:*:*:wordpress:*:*	CWE-73

Recommendations



Update Immediately: Upgrade the Forminator Forms plugin to version 1.44.3 or later. This release includes the necessary fix that eliminates the arbitrary file deletion vulnerability and should be applied as soon as possible to protect your site.



Temporarily Disable the Plugin: If you're unable to update right away, it's recommended to deactivate the Forminator plugin temporarily. Keeping it active while unpatched leaves your site exposed to exploitation.



Verify File Integrity: After updating, check the integrity of critical WordPress files, especially wp-config.php, to ensure they have not been tampered with or deleted as a result of exploitation attempts.



Review Form Submissions: Examine recent form submissions for suspicious or unexpected entries. Look for evidence of exploitation, such as submissions containing unusual file paths or file arrays in non-upload fields.



Implement Web Application Firewall (WAF): Deploy a Web Application Firewall (WAF) to monitor and filter incoming traffic. A WAF can detect and block malicious form submissions, including those using path traversal techniques to exploit the vulnerability. Enabling specific security rules related to file handling can greatly enhance your protection.



Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0040</u> Impact
<u>TA0005</u> Defense Evasion	<u>T1485</u> Data Destruction	<u>T1190</u> Exploit Public-Facing Application	<u>T1204</u> User Execution
<u>T1070</u> Indicator Removal	<u>T1588</u> Obtain Capabilities	<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities

Patch Details

Upgrade the Forminator Forms plugin to version 1.44.3 or later.

Link:

<https://wordpress.org/plugins/forminator/advanced/>

<https://www.wordfence.com/threat-intel/vulnerabilities/id/6dc9b4cb-d36b-4693-a7b9-1dad123b6639?source=cve>

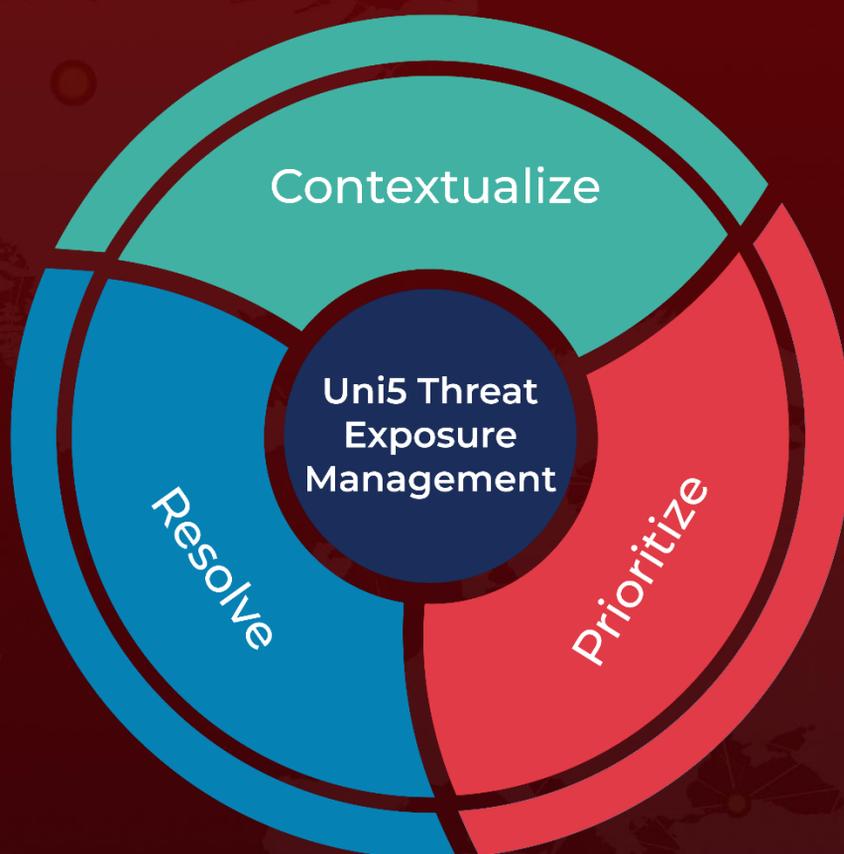
References

<https://undercodenews.com/wordpress-under-fire-critical-plugin-flaw-exposes-over-600000-sites-to-full-takeover/>

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 free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

July 3, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com